Från: [redacted]
[redacted]

kommun@ale.se; klk@alvesta.se; servicecenter@avesta.se; info; kommun@borgholm.se; registrator@bra.se; info@centrumforrattvisa.se; info@crd.org; kommun@dalsed.se; kommunen@danderyd.se; do; domstolsverket@dom.se; info@dorotea.se; huvudregistrator; kommunen@falkoping.se; kommun@filipstad.se; flenskommun@flen.se; exp-hkv; forvaltningsratteniharnosand; forvaltningsrattenimalmo; forvaltningsrattenistockholm; stadsledningskontoret@stadshuset.goteborg.se; hovratten ovrenorrland; kommun@hudiksvall.se; kommunen@hassleholm.se; registrator; imy; registrator; kommunstyrelse@jonkoping.se; kammarratten goteborg; kammarrattenistockholm; karlskrona.kommun@karlskrona.se; kommun@kiruna.se; registrator; kommun@laxa.se; lulea.kommun@lulea.se; registrator@lysekil.se; info@mobilitysweden.se; mora.kommun@mora.se; polisforbundet@polisforbundet.se; registrator kansli; Regelrådet; region@regionjh.se; region@skane.se; registrator.rlk@regionstockholm.se; region@regionostergotland.se; justitieombudsmannen@jo.se; remiss@msverige.se; kanslihuset@sjobo.se; skelleftea tingsratt; kommunen@staffanstorp.se; kommunstyrelsen@stockholm.se; registrator; kommun@sunne.se; info@advokatsamfundet.se; remiss@advokatsamfundet.se; registrator@skr.se; sakint; sakerhetspolisen@sakerhetspolisen.se; kommun@soderkoping.se; sodertalje.kommun@sodertalje.se; trafikverket; kontakt; info@tullkust.se; tullverket; Kommunledningskontoret@uppsala.se; kommunstyrelsen@vasteras.se; post@vgregion.se; registrator; kommun@amal.se; kundtjanst@are.se

Kopia: betankande@elanders.com; Ju Registrator

Ärende: Remiss av promemorian Förbättrade möjligheter för polisen att använda kamerabevakning (Ds 2024:11)

Datum: den 11 juni 2024 12:56:34

Ds: Förbättrade möjligheter för polisen att använda kamerabevakning - Regeringen.se

Remittering av promemorian Förbättrade möjligheter för polisen att använda kamerabevakning (Ds 2024:11)

Remissinstanser

1. Ale kommun
2. Alvesta kommun
3. Avesta kommun
4. Barnombudsmannen
5. Borgholms kommun
6. Brottsförebyggande rådet
7. Centrum för rättvisa
8. Civil Rights Defenders
9. Dals-Eds kommun
10. Danderyds kommun
11. Diskrimineringsombudsmannen
12. Domstolsverket
13. Dorotea kommun
14. Ekobrottsmyndigheten
15. Falköpings kommun
16. Filipstads kommun
17. Flens kommun
18. Försvarsmakten
19. Förvaltningsrätt i Härnösand
20. Förvaltningsrätten i Malmö
21. Förvaltningsrätten i Stockholm

22. Göteborgs kommun
23. Hovrätten för Övre Norrland
24. Hudiksvalls kommun
25. Hässleholms kommun
26. Institutet för mänskliga rättigheter
27. Integritetsskyddsmyndigheten
28. Justitiekanslern
29. Jönköpings kommun
30. Kammarrätten i Göteborg
31. Kammarrätten i Stockholm
32. Karlskrona kommun
33. Kiruna kommun
34. Kustbevakningen
35. Laxå kommun
36. Luleå kommun
37. Lysekils kommun
38. Mobility Sweden
39. Mora kommun
40. Polisförbundet
41. Polismyndigheten
42. Regelrådet
43. Region Jämtland Härjedalen
44. Region Skåne
45. Region Stockholm
46. Region Östergötland
47. Riksdagens ombudsmän
48. Riksförbundet M Sverige
49. Sjöbo kommun
50. Skellefteå tingsrätt
51. Staffanstorps kommun
52. Stockholms kommun
53. Stockholms universitet (Juridiska fakulteten)
54. Sunne kommun
55. Sveriges advokatsamfund
56. Sveriges Kommuner och Regioner
57. Säkerhets- och integritetsskyddsnämnden
58. Säkerhetspolisen
59. Söderköpings kommun
60. Södertälje kommun

61. Trafikverket
62. Transportstyrelsen
63. Tull-Kust
64. Tullverket
65. Uppsala kommun
66. Västerås kommun
67. Västra Götalandsregionen
68. Åklagarmyndigheten
69. Åmål kommun
70. Åre kommun

Remissvaren ska ha kommit in till Justitiedepartementet **senast den 16 september 2024**. Svaren bör lämnas per e-post till ju.remissvar@regeringskansliet.se och med kopia till Ju.L4@regeringskansliet.se. Ange diarienummer Ju2024/01351 och remissinstansens namn i ämnesraden på e-postmeddelandet.

Svaret bör lämnas i två versioner: den ena i ett bearbetningsbart format (t.ex. Word), den andra i ett format (t.ex. pdf) som följer tillgänglighetskraven enligt lagen (2018:1937) om tillgänglighet till digital offentlig service. Remissinstansens namn ska anges i namnet på respektive dokument.

Remissvaren kommer att publiceras på regeringens webbplats.

I remissen ligger att regeringen vill ha synpunkter på förslagen eller materialet i promemorian. Om remissen är begränsad till en viss del av promemorian, anges detta inom parentes efter remissinstansens namn i remisslistan. En sådan begränsning hindrar givetvis inte att remissinstansen lämnar synpunkter också på övriga delar.

Myndigheter under regeringen är skyldiga att svara på remissen. En myndighet avgör dock på eget ansvar om den har några synpunkter att redovisa i ett svar. Om myndigheten inte har några synpunkter, räcker det att svaret ger besked om detta.

För **andra remissinstanser** innebär remissen en inbjudan att lämna synpunkter.

Promemorian kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Remissinstanserna kan utan kostnad beställa tryckta exemplar av promemorian via ett beställningsformulär hos Elanders Sverige AB.

Råd om hur remissyttranden utformas finns i Statsrådsberedningens promemoria Svara på remiss (SB PM 2021:1). Den kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Charlotta Fröcklin
Ämnesråd

Kopia till

Elanders Sverige AB, e-postadress: betankande@elanders.com

Förbättrade möjligheter för polisen att använda kamerabevakning

Ds 2024:11

Regeringskansliet
Justitiedepartementet

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss
Statsrådsberedningen, *SB PM 2021:1.*
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Omslag: Regeringskansliets standard
Tryck och remisshantering: Elanders Sverige AB, Stockholm 2024

ISBN 978-91-525-0944-9 (tryck)
ISBN 978-91-525-0945-6 (pdf)
ISSN 0284-6012

Till statsrådet och chefen för Justitiedepartementet

Den 29 november 2023 beslutade chefen för Justitiedepartementet, statsrådet Gunnar Strömmer, att uppdra åt f.d. hovrättsrådet Kazimir Åberg att biträda departementet med att utreda vissa frågor som ska förbättra förutsättningarna för Polismyndigheten och Säkerhetspolisen att använda kamerabevakning i sin verksamhet (Ju 2023:D). Ämnessakkunnige Daniel Bergström förordnades samma dag som sekreterare. Den 12 februari 2024 förordnades t.f. kammarrättsassessorn Emma Lindmark som sekreterare.

Härigenom överlämnas promemorian *Förbättrade möjligheter för polisen att använda kamerabevakning*. Arbetet är i och med detta avslutat.

Täby i maj 2024

Kazimir Åberg

/Daniel Bergström
Emma Lindmark

Innehåll

Sammanfattning **11**

Summary **16**

1 Författningsförslag **21**

1.1 Förslag till lag om ändring i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning 21

1.2 Förslag till lag om ändring i kamerabevakningslagen (2018:1200) 23

1.3 Förslag till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område 25

1.4 Förslag till förordning om ändring i vägtrafikdataförordningen (2019:382) 30

2 Inledning 31

2.1 Uppdraget 31

2.2 Annat pågående arbete rörande kamerabevakning 32

2.3 Arbetets bedrivande 33

2.4 Arbetets avgränsningar 34

3 Rätten till privatliv och skyddet för den personliga integriteten 35

3.1 Inledning 35

3.2 Rättslig reglering ... 35
3.2.1 Regeringsformen ... 35
3.2.2 Europakonventionen ... 37
3.2.3 EU:s rättighetsstadga ... 39
3.2.4 Förenta nationernas (FN:s) allmänna förklaring om de mänskliga rättigheterna ... 41
3.2.5 Dataskyddskonventionen och Organisation for Economic Co-operation and Developments (OECD:s) riktlinjer ... 41
3.2.6 Barnkonventionen ... 43

3.3 Begreppet personlig integritet ... 43

4 Internationell utblick ... 49

4.1 Inledning ... 49

4.2 Användning av ANPR-teknik ... 49
4.2.1 Finland ... 49
4.2.2 Norge ... 50
4.2.3 Danmark ... 50
4.2.4 Tyskland ... 52
4.2.5 Nederländerna ... 54
4.2.6 Storbritannien ... 55
4.2.7 Italien ... 56
4.2.8 Belgien ... 57

4.3 Användning av ansiktsigenkänning ... 58
4.3.1 Finland ... 58
4.3.2 Norge ... 59
4.3.3 Danmark ... 60
4.3.4 Tyskland ... 61
4.3.5 Nederländerna ... 62
4.3.6 Storbritannien ... 63
4.3.7 Italien ... 65
4.3.8 Belgien ... 66

4.4 Polisens tillgång till material från annans kamerabevakning ... 66
4.4.1 Finland ... 66
4.4.2 Norge ... 67
4.4.3 Danmark ... 67

4.4.4 Tyskland ... 67
4.4.5 Nederländerna ... 69
4.4.6 Storbritannien ... 69
4.4.7 Italien ... 70
4.4.8 Belgien ... 70

5 Den dataskyddsrättsliga regleringen ... 71

5.1 Inledning ... 71

5.2 Den EU-rättsliga dataskyddsregleringen ... 71
5.2.1 EU:s dataskyddsreform och dataskyddsförordningen ... 71
5.2.2 Dataskyddsdirektivet ... 75
5.2.3 EU:s förordning om artificiell intelligens (AI) ... 80

5.3 Den svenska dataskyddslagstiftningen ... 81
5.3.1 Allmänt om den svenska regleringen ... 81
5.3.2 Brottsdatalagen ... 82
5.3.3 Polisens brottsdatalag ... 87
5.3.4 Säkerhetspolisens datalag ... 92

6 Kamerabevakning ... 93

6.1 Inledning ... 93

6.2 Kamerabevakningslagen ... 93
6.2.1 Särskilt om intresseavvägningen ... 97

6.3 Personuppgiftsbehandling ... 99

6.4 Kamerabevakning med ANPR-teknik ... 101

6.5 Kamerabevakning i vissa myndigheters verksamhet ... 103
6.5.1 Polismyndigheten ... 103
6.5.2 Trafikverket ... 105
6.5.3 Transportstyrelsen ... 107
6.5.4 Tullverket ... 108

7 Rättsliga förutsättningar för Polismyndigheten och Säkerhetspolisen att ta del av material från andra aktörers bevakningskameror ... 111

7.1 Inledning ... 111

7.2 Utlämnande av material från bevakningskameror med stöd av straffprocessuella tvångsmedel, m.m. ... 112

7.3 Utlämnande av material från bevakningskameror med stöd av offentlighets- och sekretesslagen ... 114
7.3.1 Generellt om sekretess ... 115
7.3.2 Sekretess för material från bevakningskameror ... 117
7.3.3 Sekretess för material från trängselskattekameror och infrastrukturavgiftskameror ... 119
7.3.4 Sekretessbrytande bestämmelser ... 119

7.4 Dataskyddsrättsliga aspekter ... 123
7.4.1 Finalitetsprincipen ... 123
7.4.2 Särskilt om informationsskyldighet ... 126

8 Hantering och användning av material från kamerabevakning i trafiken ... 129

8.1 Inledning ... 129

8.2 Material från trafiksäkerhetskameror ... 129

8.3 Material från kameror vid betalstationer och kontrollpunkter för trängselskatt och infrastrukturavgift ... 130
8.3.1 Transportstyrelsen ... 130
8.3.2 Skatteverket ... 132

9 Polismyndighetens tillgång till material från andras bevakningskameror ... 135

9.1 Inledning ... 135

9.2 Elektroniskt informationsutbyte ... 135

9.3 Polismyndighetens tillgång till material från kamerabevakning genom samverkan ... 138
9.3.1 SOT-lösningen ... 138

9.4 Olika sätt för Polismyndigheten att ta del av material från andra offentliga aktörers bevakningskameror ... 144

10 Ansiktsigenkänning ... 147

10.1 Inledning ... 147

10.2 Biometriska uppgifter ... 148
10.2.1 Begreppet biometriska uppgifter ... 148
10.2.2 Behandling av biometriska uppgifter ... 148

10.3 Polismyndighetens användning av ansiktsigenkänning ... 150
10.3.1 Särskilt om ”krunchning” ... 152

10.4 EU:s AI-förordning ... 154

11 Överväganden ... 157

11.1 Inledning ... 157

11.2 En ny reglering för kamerabevakning på platser som allmänt används för trafik med motorfordon ... 159
11.2.1 Polismyndigheten och Säkerhetspolisen ska få bedriva kamerabevakning på platser som allmänt används för trafik med motorfordon utan att det föregås av en dokumenterad intresseavvägning ... 162
11.2.2 En ny reglering om behandling av personuppgifter som samlats in av Polismyndigheten och Säkerhetspolisen genom kamerabevakning på platser som allmänt används för trafik med motorfordon ... 168

11.3 Inget avskaffat krav på upplysning om kamerabevakning på platser som allmänt används för trafik med motorfordon ... 176

11.4 Polismyndigheten och Säkerhetspolisen får i vissa fall ges tillstånd att använda system för biometrisk fjärridentifiering i realtid på allmän plats för brottsbekämpningsändamål ... 178

11.5 Användning av teknik som extraherar information i bildmaterial från kamerabevakning ... 183

11.6 En utvidgad uppgiftsskyldighet för Transportstyrelsen avseende uppgifter från trängselskattekameror och infrastrukturavgiftskameror ... 185

11.7 Uppgifter från kamerabevakning ska kunna göras gemensamt tillgängliga 189

11.8 Längsta tid för behandling av gemensamt tillgängliga uppgifter som samlats in genom kamerabevakning..... 195

11.9 Tydligare reglering av möjligheterna att dela personuppgifter som samlats in från kamerabevakning med Polismyndigheten och Säkerhetspolisen..... 199

12 Ikraftträdande- och övergångsbestämmelser..... 205

12.1 Ikraftträdandebestämmelser 205

12.2 Övergångsbestämmelser 206

13 Förslagens konsekvenser..... 209

13.1 Inledning 209

13.2 Ekonomiska konsekvenser..... 209
13.2.1 Polismyndigheten och Säkerhetspolisen 209
13.2.2 Integritetsskyddsmyndigheten 212
13.2.3 Transportstyrelsen 213
13.2.4 Trafikverket 213
13.2.5 Domstols- och åklagarväsendena 213
13.2.6 Enskilda aktörer 214

13.3 Konsekvenser för den personliga integriteten och andra grundläggande fri- och rättigheter..... 214

13.4 Konsekvenser för det brottsbekämpande arbetet..... 217

14 Författningskommentar..... 219

14.1 Förslaget till lag om ändring i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning 219

14.2 Förslaget till lag om ändring i kamerabevakningslagen (2018:1200) 221

14.3 Förslaget till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område 222

Bilaga 1 Uppdragsbeskrivning 231

Bilaga 2 Europaparlamentets ståndpunkt fastställd vid första behandlingen den 13 mars 2024 inför antagandet av Europaparlamentets och rådets förordning (EU) 2024/… om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (rättsakt om artificiell intelligens) 237

Sammanfattning

I denna promemoria lämnas förslag som syftar till förbättrade förutsättningar för Polismyndigheten och Säkerhetspolisen att använda kamerabevakning i sin verksamhet.

Nedan följer en kortfattad beskrivning av de lämnade förslagen.

Polismyndigheten och Säkerhetspolisen ska få bedriva kamerabevakning på platser som allmänt används för trafik med motorfordon utan att användningen föregås av en dokumenterad intresseavvägning

Polismyndigheten och Säkerhetspolisen ges möjlighet att bedriva kamerabevakning på vägar, gator, torg och annan led eller plats som allmänt används för trafik med motorfordon utan att dessförinnan behöva göra en dokumenterad intresseavvägning. Syftet är att effektivisera Polismyndighetens och Säkerhetspolisens brottsbekämpande arbete, och att möjliggöra en bredare användning av ANPR-teknik (*automatic number plate recognition*), vilket enligt den analys som görs i denna promemoria är viktig för att bekämpa den grova brottsligheten.

Att Polismyndigheten och Säkerhetspolisen får bedriva kamerabevakning på platser som allmänt används för trafik med motorfordon utan att en intresseavvägning först görs innebär inte att bevakningen är oreglerad. Kamerabevakningen måste ske i överensstämmelse med övrig dataskyddsrättslig reglering. Det måste t.ex. finnas en rättslig grund för den behandling av personuppgifter som bevakningen innebär. Utöver rättslig grund måste insamlingen även ske för ett konkret ändamål i varje specifikt fall.

En ny reglering om behandling av personuppgifter som samlats in av Polismyndigheten och Säkerhetspolisen genom kamerabevakning på platser som allmänt används för trafik med motorfordon

För att väga upp den integritetsförlust som en utökning av möjligheterna till kamerabevakning innebär införs en begränsning av vilka personuppgifter som får användas samt för vilka ändamål och hur länge användningen får ske. Detta sker genom att en ny rättslig grund införs för behandling av sådana uppgifter. Personuppgifter som har samlats in genom kamerabevakning på platser som allmänt används för trafik med motorfordon och som rör fordon får behandlas av Polismyndigheten eller Säkerhetspolisen endast om syftet med behandlingen är att förebygga, förhindra, upptäcka, utreda eller lagföra brott för vilket det är föreskrivet fängelse i tre år eller mer. Materialet får alltid behandlas i sex månader efter att det har samlats in. Detta gäller dock inte för personuppgifter i form av bilder av enskilda.

Uppgifterna får användas så länge användningen sker för ändamål som anges i bestämmelsen. Efter att den angivna tiden har gått ut får möjligheten att fortsätta att använda uppgifterna avgöras med stöd av annan tillämplig dataskyddsrättslig reglering.

Polismyndigheten och Säkerhetspolisen får i vissa fall ges tillstånd att använda system för biometrisk fjärridentifiering i realtid på allmän plats för brottsbekämpningsändamål

Polismyndigheten och Säkerhetspolisen ges möjlighet att i vissa fall få tillstånd att använda system för biometrisk fjärridentifiering i realtid på allmän plats för brottsbekämpningsändamål. Tillstånd får ges endast i den mån sådan användning är absolut nödvändig och för de ändamål som anges i artikel 5.1 h i EU:s kommande AI-förordning[1]. Dessa ändamål är följande.

[1] Europaparlamentets ståndpunkt fastställd vid första behandlingen den 13 mars 2024 inför antagandet av Europaparlamentets och rådets förordning (EU) 2024/… om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (rättsakt om artificiell intelligens).

i. Målinriktad sökning efter specifika offer för människorov, människohandel eller sexuellt utnyttjande av människor, samt sökning efter försvunna personer.

ii. Förhindrande av ett specifikt, betydande och överhängande hot mot fysiska personers liv eller fysiska säkerhet eller ett verkligt och aktuellt eller verkligt och förutsebart hot om en terroristattack;

iii. Lokalisering eller identifiering av en person som misstänks ha begått ett brott, i syfte att genomföra en brottsutredning, lagföring eller ett verkställande av en straffrättslig påföljd för brott som avses i bilaga II och som i den berörda medlemsstaten kan leda till fängelse eller annan frihetsberövande åtgärd under en längsta tidsperiod på minst fyra år.

När det gäller tillämpningen av denna regel såvitt gäller artikel 5.1 h iii får en bedömning göras om de brott som är upptagna i förordningens bilaga har en motsvarighet i svensk rätt.

För att den regel som här föreslås ska kunna träda i kraft krävs att förordningen träder i kraft och att ytterligare bestämmelser införs. Det är fråga om bl.a. föreskrifter om vilken myndighet som ska lämna tillstånd för användningen av system för biometrisk fjärridentifiering i realtid.

Tydligare möjligheter att dela personuppgifter som samlats in från kamerabevakning med Polismyndigheten och Säkerhetspolisen

Det införs en ny rättslig grund för vidarebehandling av personuppgifter i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Den rättsliga grunden ger privata och offentliga aktörer en möjlighet att – på begäran av Polismyndigheten och Säkerhetspolisen – behandla personuppgifter som samlats in genom kamerabevakning för att lämna sådana uppgifter som begärs av respektive myndighet för att utreda ett begånget brott för vilket fängelse är föreskrivet eller för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket fängelse är föreskrivet.

Bestämmelsen innebär bl.a. att aktörer som får en förfrågan om utlämnande av personuppgifter som samlats in från kamerabevakning från Polismyndigheten eller Säkerhetspolisen inte behöver göra några närmare överväganden om personuppgiftsbehandlingens förenlighet med finalitetsprincipen. Bestämmelsen utgör dock ingen skyldighet att behandla eller lämna ut personuppgifter på en begäran från Polismyndigheten eller Säkerhetspolisen.

En utvidgad uppgiftsskyldighet för Transportstyrelsen om uppgifter från trängselskattekameror och infrastrukturavgiftskameror

Det föreslås en bestämmelse enligt vilket Transportstyrelsen, på begäran av Polismyndigheten eller Säkerhetspolisen, utan dröjsmål ska lämna ut uppgifter om trängselskatt eller infrastrukturavgift som gäller passager av en betalstation eller kontrollpunkt, om det av begäran framgår att uppgifterna behövs i ett brådskande fall för att förebygga, förhindra, upptäcka eller utreda ett brott för vilket det är föreskrivet fängelse i tre år eller mer eller ett straffbart försök eller en straffbar förberedelse eller stämpling till eller underlåtenhet att avslöja eller förhindra sådant brott.

Uppgifter från kamerabevakning ska kunna göras gemensamt tillgängliga

Uppgifter som samlats in genom kamerabevakning med stöd av kamerabevakningslagen (2018:1200) eller annan författning ska få göras gemensamt tillgängliga. Tillgången till sådana uppgifter ska begränsas till särskilt angivna tjänstemän som är i behov av uppgifterna för att upprätthålla allmän ordning och säkerhet eller förebygga, förhindra, upptäcka eller utreda och lagföra ett brott för vilket är föreskrivet fängelse i tre år eller mer. Uppgifterna får behandlas i sex månader från det att de samlades in.

Genom att personuppgifter som samlats in genom kamerabevakning görs gemensamt tillgängliga kan Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket medges direkt-

åtkomst i vissa fall till uppgifterna. En bestämmelse om direktåtkomst reglerar endast formen för utlämnande av uppgifter och är inte sekretessbrytande. Direktåtkomst kan därför endast medges till uppgifter som inte omfattas av sekretess.

Summary

In this memorandum, proposals are made aimed at improving the conditions for the Swedish Police Authority and the Swedish Security Service to use camera surveillance in their operations.

The following is a brief description of the submitted proposals.

The Swedish Police Authority and the Swedish Security Service shall be allowed to conduct camera surveillance in places that are commonly used for traffic with motor vehicles without the use being preceded by a documented balance of interests

The Swedish Police Authority and the Swedish Security Service are given the opportunity to conduct camera surveillance on roads, streets, squares and other routes or places that are commonly used for traffic with motor vehicles without having to make a documented balance of interests. The aim is to streamline the law enforcement work of the Swedish Police Authority and the Swedish Security Service, and to enable a wider use of automatic number plate recognition (ANPR) technology, which, according to the analysis made in this memorandum, is important for combating serious crime.

The fact that the Swedish Police Authority and the Swedish Security Service may conduct camera surveillance in places that are commonly used for traffic with motor vehicles without a balance of interests first being made does not mean that the surveillance is unregulated. The camera surveillance must be carried out in accordance with other data protection regulations. For example, there must be a legal basis for the processing of personal data that

the monitoring entails. In addition to the legal basis, the collection must also take place for a specific purpose in each specific case.

A new regulation on the processing of personal data collected by the Swedish Police Authority and the Swedish Security Service through camera surveillance in places commonly used for traffic with motor vehicles

In order to compensate for the loss of privacy that an extension of the possibilities for camera surveillance entails, a restriction is introduced on which personal data may be used and for what purposes and for how long the use may take place. This is done by introducing a new legal basis for the processing of such data. Personal data that relates to vehicles may be processed by the Swedish Police Authority or the Swedish Security Service only if the purpose of the processing is to prevent, detect, investigate or prosecute crimes for which there is a prescribed prison term of three years or more. The data may always be processed for six months after it has been collected. However, this does not apply to personal data in the form of images of individuals.

The data may be used as long as the use is made for the purpose specified in the provision. After the specified time has expired, the possibility of continuing to use the data may be determined by other applicable data protection legislation.

The Swedish Police Authority and the Swedish Security Service may in some cases be granted permission to use systems for biometric remote identification in real-time in public places for law enforcement purposes

The Swedish Police Authority and the Swedish Security Service are given the opportunity to in some cases obtain permission to use systems for biometric remote identification in real-time in public places for the purposes of law enforcement. Authorisation may be granted only to the extent that such use is strictly necessary and for

the purposes set out in Article 5.1 h of the upcoming EU AI Act[2]. These purposes are as follows.

i. Targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as search for missing persons.

ii. The prevention of a specific, significant, and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack.

iii. The location or identification of a person suspected of having committed a criminal offense for the purpose of conducting a criminal investigation, prosecution or executing of a criminal penalty for offenses referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

As regards the application of this rule as regards Article 5.1 h iii, an assessment may be made whether the offenses listed in the Annex to the AI Act have a counterpart in Swedish law.

The entry into force of the proposed rule requires the entry into force of the AI Act and the introduction of additional provisions. These include regulations on who should grant authorization for the use of biometric remote identification systems in real-time.

Clearer possibilities to share personal data collected through camera surveillance with the Swedish Police Authority and the Swedish Security Service

A new legal basis for the further processing of personal data is introduced in the Act (2018:218) with additional provisions to the EU Data Protection Regulation. The legal basis provides private and public actors with the opportunity to – at the request of the Swedish

[2] Position of the European Parliament adopted at first reading on 13 March 2024 with a view to the adoption of Regulation (EU) 2024/… of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

Police Authority and the Swedish Security Service – process personal data collected through camera surveillance in order to provide such data as is requested by the respective authority to investigate a committed crime for which imprisonment is prescribed or to investigate, prevent or detect criminal activities involving offenses for which imprisonment is prescribed.

The provision means, among other things, that actors who receive a request for the disclosure of personal data collected through camera surveillance from the Swedish Police Authority or the Swedish Security Service do not need to make any further considerations about the compatibility of the personal data processing with the finality principle. However, this provision does not constitute an obligation to process or disclose personal data at the request of the Swedish Police Authority or the Swedish Security Service.

An extended data obligation for the Swedish Transport Agency on data from congestion tax cameras and infrastructure fee cameras

A provision is proposed under which the Swedish Transport Agency, at the request of the Swedish Police Authority or the Swedish Security Service, shall without delay disclose information on congestion tax or infrastructure charge relating to the passage of a payment station or control point, if the request indicates that the information is needed in an urgent case to prevent, detect or investigate a crime for which there is a prescribed prison term of three years or more or a punishable attempt or a punishable preparation or stamping of, or failure to disclose or prevent, such a crime.

Data from camera surveillance should be made jointly available

Information collected through camera surveillance under the Swedish Camera Surveillance Act (2018:1200) or other regulations may be made jointly available. Access to such information shall be limited to designated officials who need the information for the purposes of maintaining public order and security, preventing,

detecting or investigating and prosecuting a crime for which a prison sentence of three years or more is prescribed. The data may be processed for six months from the date of their collection.

By making personal data collected through camera surveillance available jointly, the Swedish Police Authority, the Swedish Security Service, the Swedish Economic Crime Authority, the Swedish Public Prosecutor's Office, the Swedish Customs, the Swedish Coast Guard and the Swedish Tax Agency can be granted direct access to the data in some cases. A provision on direct access only regulates the form of disclosure of data and is not a breach of confidentiality. Direct access can therefore only be granted to data that is not covered by confidentiality.

1 Författningsförslag

1.1 Förslag till lag om ändring i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

Härigenom föreskrivs i fråga om lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

dels att det ska införas en ny paragraf, 2 kap. 5 §, med följande lydelse,

dels att det närmast före 2 kap. 5 § ska införas en ny rubrik med följande lydelse

Nuvarande lydelse	*Föreslagen lydelse*
	2 kap.
	Möjligheter för enskilda att lämna uppgifter som samlats in från kamerabevakning till Polismyndigheten och Säkerhetspolisen
	5 § *Enskilda får behandla personuppgifter som samlats in från kamerabevakning för att lämna sådana uppgifter som begärs av*

Polismyndigheten eller Säkerhetspolisen för att utreda ett begånget brott för vilket fängelse är föreskrivet eller för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket fängelse är föreskrivet.

Denna lag träder i kraft den 1 januari 2025.

1.2 Förslag till lag om ändring i kamerabevakningslagen (2018:1200)

Härigenom föreskrivs att 14 c § kamerabevakningslagen (2018:1200) ska ha följande lydelse

Nuvarande lydelse	*Föreslagen lydelse*
14 c §[1]	
Bestämmelserna i 14 a och 14 b §§ gäller inte vid	
1. kamerabevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning,	
2. kamerabevakning som Kustbevakningen, Polismyndigheten, Säkerhetspolisen eller Tullverket bedriver i fall som avses i 9 § 2 och 6–10 *och*	2. kamerabevakning som Kustbevakningen, Polismyndigheten, Säkerhetspolisen eller Tullverket bedriver i fall som avses i 9 § 2 och 6–10,
3. kamerabevakning som Kustbevakningen, Polismyndigheten, Säkerhetspolisen eller Tullverket bedriver i gränsnära områden som avses i 2 § lagen (2023:474) om polisiära befogenheter i gränsnära områden, eller av tillfartsvägar till sådana gränsnära områden som avses i 2 § 3 eller 4 samma lag, om bevakningen bedrivs inom 20 kilometer från området.	3. kamerabevakning som Kustbevakningen, Polismyndigheten, Säkerhetspolisen eller Tullverket bedriver i gränsnära områden som avses i 2 § lagen (2023:474) om polisiära befogenheter i gränsnära områden, eller av tillfartsvägar till sådana gränsnära områden som avses i 2 § 3 eller 4 samma lag, om bevakningen bedrivs inom 20 kilometer från området *och*
	4. *annan kamerabevakning som Polismyndigheten eller Säkerhetspolisen bedriver av väg, gata, torg och annan led eller*

[1] Senaste lydelse SFS 2023:477.

plats som allmänt används för trafik med motorfordon.

Denna lag träder i kraft den 1 januari 2025.

1.3 Förslag till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område

Härigenom föreskrivs i fråga om lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område

dels att 2 kap. 2 §, 3 kap. 2 §, 4 kap. 6, 12 och 13 §§ ska ha följande lydelse,

dels att det ska införas tre nya paragrafer, 2 kap. 1 a och 4 a §§ samt 4 kap. 11 a §, med följande lydelse

Nuvarande lydelse	*Föreslagen lydelse*
	2 kap.
	1 a §
	Personuppgifter som rör motorfordon och som har samlats in genom kamerabevakning som bedrivs med stöd av 14 c § 4 kamerabevakningslagen (2018:1200) får behandlas av Polismyndigheten och Säkerhetspolisen endast om syftet med behandlingen är att förebygga, förhindra, upptäcka, utreda eller lagföra brott för vilket det är föreskrivet fängelse i tre år eller mer. Sådan behandling får alltid ske i sex månader efter det att uppgifterna samlades in.
	Första stycket gäller inte för personuppgifter i form av bilder av enskilda.
	2 §
Förutsättningarna för att behandla personuppgifter som behandlas med stöd av *1 §* för nya	Förutsättningarna för att behandla personuppgifter som behandlas med stöd av 1 *eller 1 a §*

ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:1177).	för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:1177).
	4 a § *Polismyndigheten och Säkerhetspolisen får ges tillstånd att använda system för biometrisk fjärridentifiering i realtid på allmän plats under de förutsättningar och för de syften som anges i artikel 5.1 h EU:s förordning om artificiell intelligens*[1]*.*

3 kap.

2 §[2]

Följande personuppgifter får göras gemensamt tillgängliga:

1. Uppgifter som kan antas ha samband med misstänkt brottslig verksamhet, om den misstänkta verksamheten

   a) innefattar brott för vilket det är föreskrivet fängelse i ett år eller mer, eller

   b) sker systematiskt.

2. Uppgifter som behövs för övervakningen av en person som

   a) kan antas komma att begå brott för vilket det är föreskrivet fängelse i två år eller mer, och

   b) är allvarligt kriminellt belastad eller kan antas utgöra ett hot mot andras personliga säkerhet.

3. Uppgifter som förekommer i ett ärende om utredning av eller lagföring för brott.

---

[1] Europaparlamentets ståndpunkt fastställd vid första behandlingen den 13 mars 2024 inför antagandet av Europaparlamentets och rådets förordning (EU) 2024/… om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (rättsakt om artificiell intelligens).

[2] Senaste lydelse SFS 2019:435.

4. Uppgifter som förekommer i ett ärende om uppbörd.
5. Uppgifter som förekommer i ett ärende om kontaktförbud eller om personskydd.
6. Uppgifter som har rapporterats till Polismyndighetens ledningscentraler.
7. Uppgifter som behandlas i syfte att upprätthålla allmän ordning och säkerhet.
8. Uppgifter som behandlas i syfte att fullgöra internationella åtaganden, om det krävs för att den aktuella förpliktelsen ska kunna fullgöras.
9. *Uppgifter som har samlats in genom kamerabevakning med stöd av kamerabevakningslagen (2018:1200) eller annan författning.*

Dna-profiler får inte göras gemensamt tillgängliga. Att sådana uppgifter får behandlas i särskilda register följer av 5 kap.

Tillgången till uppgifter som görs gemensamt tillgängliga med stöd av första stycket 2 ska begränsas till särskilt angivna tjänstemän som har till uppgift att arbeta med övervakningen. Information om att en person är föremål för övervakning får dock göras tillgänglig för andra.

Tillgången till uppgifter som görs gemensamt tillgängliga med stöd av första stycket 9 ska begränsas till särskilt angivna tjänstemän som är i behov av uppgifterna för att upprätthålla allmän ordning och säkerhet eller förebygga, förhindra, upptäcka eller utreda och lagföra brott för vilket det är föreskrivet fängelse i tre år eller mer.

4 kap.

6 §[3]

Personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § första stycket 1, 2 eller *5–8* får som längst behandlas under den tid som anges i *7–11 §§*.	Personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § första stycket 1, 2 eller *5–9* får som längst behandlas under den tid som anges i *7–11 a §§*.
Bestämmelsen i 2 kap. 17 § andra stycket brottsdatalagen (2018:1177) gäller inte vid tillämpningen av *7–11 §§*.	Bestämmelsen i 2 kap. 17 § andra stycket brottsdatalagen (2018:1177) gäller inte vid tillämpningen av *7–11 a §§*.
	11 a § *Personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § första stycket 9 får inte behandlas längre än sex månader efter det att de samlades in.*

12 §

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att vissa kategorier av personuppgifter får fortsätta att behandlas för ändamål inom denna lags tillämpningsområde under längre tid än vad som anges i 3, 4 eller *7–11* §.	Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att vissa kategorier av personuppgifter får fortsätta att behandlas för ändamål inom denna lags tillämpningsområde under längre tid än vad som anges i 3, 4 eller *7–11 a* §.

13 §

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

[3] Senaste lydelse SFS 2019:435.

1. att personuppgifter får behandlas för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål under längre tid än vad som anges i 2 § första stycket eller *7–11* §, och	1. att personuppgifter får behandlas för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål under längre tid än vad som anges i 2 § första stycket eller *7–11 a* §, och
2. begränsning av behandlingen av personuppgifter för ändamål inom denna lags tillämpningsområde vid digital arkivering.	2. begränsning av behandlingen av personuppgifter för ändamål inom denna lags tillämpningsområde vid digital arkivering.

Denna lag träder i kraft den dag regeringen bestämmer i fråga om 2 kap. 4 a § och i övrigt den 1 januari 2025.

1.4 Förslag till förordning om ändring i vägtrafikdataförordningen (2019:382)

Härigenom föreskrivs att 5 kap. 3 a § vägtrafikdataförordningen (2019:382) ska ha följande lydelse

Nuvarande lydelse	*Föreslagen lydelse*
	5 kap.
	3 a §[1]
Transportstyrelsen ska på begäran av Polismyndigheten eller Säkerhetspolisen utan dröjsmål lämna ut uppgifter om trängselskatt som gäller passager av en betalstation eller kontrollpunkt om det av begäran framgår att uppgifterna *i ett brådskande fall behövs för att förhindra eller på annat sätt ingripa mot en handling som kan utgöra terroristbrott enligt 4 § terroristbrottslagen (2022:666) eller försök, förberedelse eller stämpling till eller underlåtenhet att avslöja eller förhindra sådant brott.*	Transportstyrelsen ska på begäran av Polismyndigheten eller Säkerhetspolisen utan dröjsmål lämna ut uppgifter om trängselskatt *eller infrastrukturavgift* som gäller passager av en betalstation eller kontrollpunkt om det av begäran framgår att uppgifterna *behövs i ett brådskande fall för att förebygga, förhindra, upptäcka eller utreda ett brott för vilket det är föreskrivet fängelse i tre år eller mer, eller ett straffbart försök eller en straffbar förberedelse eller stämpling till eller underlåtenhet att avslöja eller förhindra sådant brott.*

Denna lag träder i kraft den 1 januari 2025.

[1] Senaste lydelse SFS 2022:699.

2 Inledning

2.1 Uppdraget

Uppdraget består i att förbättra förutsättningarna för Polismyndigheten och Säkerhetspolisen att använda kamerabevakning i sin verksamhet. Uppdragsbeskrivningen finns i *bilaga 1*.

Uppdraget omfattar bl.a. att lämna författningsförslag som gör att polisen i större utsträckning och på ett verkningsfullt sätt kan använda teknik som innebär kamerabevakning med automatisk igenkänning av fordons registreringsnummer (*automatic number plate recognition*, ANPR). I uppdraget ingår även att analysera om det finns förutsättningar att låta polisen i större utsträckning använda teknik som innebär kamerabevakning med automatisk ansiktsigenkänning och, om sådana förutsättningar finns, lämna författningsförslag som möjliggör ett effektivt och ändamålsenligt användande av tekniken. Slutligen omfattar uppdraget att analysera och lämna författningsförslag som gör att Polismyndigheten och Säkerhetspolisen i fler fall kan få ta del av kamerabevakningsmaterial från annans bevakning, t.ex. material från kamerasystem kopplade till statlig transportinfrastruktur eller från kommuners och regioners kamerabevakning.

I uppdragsbeskrivningen framhålls att en allmän utgångspunkt för arbetets bedrivande är att Polismyndighetens och Säkerhetspolisens möjligheter att använda sig och på andra sätt dra nytta av kamerabevakning behöver förbättras.

2.2 Annat pågående arbete rörande kamerabevakning

Flera andra arbeten har pågått parallellt med detta arbete som på olika sätt har relevans för frågan om polisens kamerabevakning.

Den 25 oktober 2023 gav regeringen Polismyndigheten, Trafikverket och Transportstyrelsen i uppdrag att lämna förslag på hur Polismyndigheten, inom ramen för befintligt regelverk, kan ges ökad tillgång till befintliga kamerasystem kopplade till den statliga transportinfrastrukturen. Detta arbete redovisades till Regeringskansliet den 6 mars 2024.

Den 23 mars 2023 gav regeringen en särskild utredare i uppdrag att föreslå åtgärder för att underlätta kamerabevakning för kommuner, regioner och andra än myndigheter som utför en uppgift av allmänt intresse. Utredningen – 2023 års kamerabevakningsutredning – fick också i uppdrag att se över utformningen av den lagstadgade intresseavvägningen i kamerabevakningslagen, för att denna bättre ska svara mot behovet av att kamerabevaka i syfte att bekämpa brott och upprätthålla allmän ordning och säkerhet. Genom tilläggsdirektiv den 28 december 2023 fick utredningen även i uppdrag bl.a. att, utifrån en kartläggning av Polismyndighetens behov, lämna förslag som innebär att Polismyndigheten i fler fall undantas från kravet på upplysning och rätten till information vid kamerabevakning (skyltningskravet). Utredningen överlämnade sitt betänkande den 15 april 2024 (SOU 2024:27, *Kamerabevakning i offentlig verksamhet*). I betänkandet föreslås bl.a. en ändrad systematik i fråga om förutsättningar för kamerabevakning, en särskild intresseavvägning för kamerabevakning i brottsbekämpande verksamhet, samt utvidgade och nya tillfälliga undantag från att tillämpa intresseavvägningen i brottsbekämpande verksamhet.

Den 12 maj 2023 gav regeringen en särskild utredare i uppdrag att utreda Säkerhetspolisens informationshantering. Uppdraget omfattar att göra en översyn av de bestämmelser som reglerar Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet. Syftet med utredningen är att skapa ändamålsenliga regler som är anpassade efter dagens behov och möjligheter. Av direktiven framgår att utgångspunkten för arbetet är att Säkerhetspolisen bör ges ökade möjligheter att behandla personuppgifter, särskilt vad gäller att samla in, sortera, lagra, bearbeta och analysera information

med hjälp av tekniska hjälpmedel. Utredningen ska redovisa sitt uppdrag senast den 15 november 2024.

Inom Europeiska unionen (EU) har arbete pågått med att förhandla EU:s nya förordning om artificiell intelligens (den s.k. AI-förordningen[8]), som bl.a. rör frågor med anknytning till kamerabevakning i form av förutsättningar för användning av ansiktsigenkänning med hjälp av AI i vissa fall. Den 13 mars 2024 antogs texten till den kommande AI-förordningen. Förordningen kommer att träda i kraft gradvis. De första delarna av förordningen, inklusive de delar som gäller förbud mot användning och begränsningar av ansiktsigenkänningsteknik i vissa fall, träder i kraft under hösten 2024.

2.3 Arbetets bedrivande

Uppdraget har inrymt ett flertal frågor av inte helt enkel natur som måst lösas på en förhållandevis kort tid. Under arbetets gång har upplysningar inhämtats från Integritetsskyddsmyndigheten, Polismyndigheten, Säkerhetspolisen, Trafikverket, Transportstyrelsen och Tullverket. Detta har skett dels i form av en löpande dialog per telefon och e-post, dels i form av möten med dels Polismyndigheten och Säkerhetspolisen, dels Trafikverket, Transportstyrelsen och Tullverket och slutligen dels Integritetsskyddsmyndigheten.

Vidare har det skett underhandskontakter och utbyte av information och underlag med sekretariatet i 2023 års kamerabevakningsutredning. Det har även skett kontakter med de tjänstemän vid Polismyndigheten som ansvarat för att samordna regeringsuppdraget om ökad tillgång till befintliga kamerasystem.

Slutligen har upplysningar om motsvarande förhållanden inhämtats från en rad jämförbara länder, nämligen Finland, Norge, Danmark, Tyskland, Nederländerna, Frankrike, Storbritannien, Belgien och Italien. Som ett led i detta inhämtande har det även förekommit digitala möten med polistjänstemän från andra europeiska länder.

[8] Europaparlamentets ståndpunkt fastställd vid första behandlingen den 13 mars 2024 inför antagandet av Europaparlamentets och rådets förordning (EU) 2024/… om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (rättsakt om artificiell intelligens).

2.4 Arbetets avgränsningar

Det framgår redan av uppdragsbeskrivningen att det inte ingår i utredningsuppdraget att överväga eller föreslå ändringar i bestämmelserna om hemlig kameraövervakning i 27 kap. rättegångsbalken, RB, eller i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

Oaktat att EU:s AI-förordning ännu inte har trätt i kraft lämnas ett förslag som möjliggör att tillstånd kan lämnas till användning av ansiktsigenkänning i realtid i vissa begränsade fall. Lagändringen i den delen föreslås träda i kraft den dag som regeringen bestämmer.

3 Rätten till privatliv och skyddet för den personliga integriteten

3.1 Inledning

Rätten till privatliv och skyddet för den personliga integriteten är två mänskliga rättigheter som skyddas i svensk grundlag och i olika folkrättsliga dokument samt EU-rättsakter. Rättigheterna har ansetts ha ett sådant skyddsvärde att de bör omfattas av ett särskilt starkt skydd mot omotiverade ingrepp. Vad som innefattas i begreppet personlig integritet påverkas av bl.a. samhällsutvecklingen och kan förändras över tid. I avsnittet redogörs för den rättsliga regleringen avseende rätten till privatliv och skyddet för den personliga integriteten samt några reflektioner kring diskussionen kring begreppet personlig integritet.

3.2 Rättslig reglering

3.2.1 Regeringsformen

Enligt 1 kap. 2 § första stycket RF ska den offentliga makten utövas med respekt för alla människors lika värde och för den enskilda människans frihet och värdighet. Av fjärde stycket i samma paragraf följer bl.a. att det allmänna ska värna den enskildes privatliv och familjeliv.

Bestämmelser om grundläggande fri- och rättigheter, inbegripet skydd mot kränkningar av den fysiska och psykiska integriteten, finns i 2 kap. RF. I 2 kap. 6 § andra stycket finns, sedan 2010 års grundlagsreform, en uttrycklig bestämmelse om skydd för den personliga integriteten. Av bestämmelsen följer att var och en är, gentemot det allmänna, skyddad mot betydande intrång i den

personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Bestämmelsen är teknikneutral och tar sikte på att skydda den personliga integriteten mot intrång som kan anses vara särskilt känsliga (jfr prop. 2009/10:80 s. 177). Vad som utgör ett betydande intrång i den personliga integriteten får bedömas utifrån åtgärdens intensitet eller omfattning samt uppgifternas integritetskänsliga natur (a. prop. s. 182 f.).

Avgörande för om en åtgärd ska anses innebära övervakning eller kartläggning av den enskildes personliga förhållanden är inte åtgärdens huvudsakliga syfte, utan vilken effekt den har (a. prop. s. 181). Vad som avses med övervakning respektive kartläggning får bedömas med utgångspunkt i vad som enligt normalt språkbruk läggs i dessa begrepp (a. prop. s. 250).

Uttrycket ”enskilds personliga förhållanden” är avsett att ha samma innebörd som i tryckfrihetsförordningen och offentlighets- och sekretesslagen. Vägledning för vad som kan läggas i uttryckets betydelse kan hämtas från normalt språkbruk (jfr prop. 1975/76:160 s. 109 och prop. 1979/80:2 s. 84). Allmänt kan sägas att personliga förhållanden avser information som är knuten till den enskildes person, t.ex. uppgifter om namn och andra personliga identifikationsuppgifter, adress, familjeförhållanden, hälsa, vandel, en persons ekonomi och fotografisk bild (se prop. 2009/10:80 s. 177).

I samband med att regeln om skydd för den personliga integriteten infördes i 2 kap. 6 § andra stycket RF avskaffades en regel som tidigare fanns i 2 kap. 3 § andra stycket RF, som infördes år 1988, av vilken följde att varje medborgare, i den utsträckning som närmare angavs i lag, skulle skyddas mot att dennes personliga integritet kränktes genom att uppgifter om vederbörande registrerades med hjälp av automatisk databehandling. Bestämmelsen syftade till att ställa upp ett konstitutionellt krav på att det skulle finnas en allmän dataskyddslagstiftning. Eftersom grundlagstiftaren bedömde att den nya bestämmelsen i 2 kap. 6 § andra stycket tillhandahöll ett skydd för den personliga integriteten som var mer verkningsfullt än det som följde av 2 kap. 3 § andra stycket avskaffades sistnämnda bestämmelse.

Enligt 2 kap. 20 § RF får rättigheterna i 2 kap. 6 § begränsas genom lag. I 2 kap. 21 § RF föreskrivs att en begränsning bara får

göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle och får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. I paragrafen föreskrivs också att begränsningen inte får göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

3.2.2 Europakonventionen

Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) tillkom inom ramen för Europarådet och innehåller bestämmelser om mänskliga och medborgerliga fri- och rättigheter. Konventionen ratificerades av Sverige år 1952 och gäller sedan år 1995 som svensk lag (lagen [1994:1219] om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna). Sedan år 1995 gäller också, enligt nuvarande 2 kap. 19 § RF, att lag eller annan föreskrift inte får meddelas i strid med Europakonventionen. Därmed har Europakonventionen indirekt konstitutionell kraft även i den interna svenska rättsordningen.

Artikel 8.1 i konventionen stadgar att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Det är huvudsakligen denna konventionsrättighet som har relevans för frågan om skyddet för den personliga integriteten.

Rätten till privatliv i konventionsrättslig mening saknar en klar avgränsad definition. Begreppet får sitt närmare innehåll genom Europadomstolens rättspraxis. Åtskilliga av de rättigheter som behandlas i andra artiklar i konventionen kan också sägas beröra privatlivet. Tortyr och omänsklig eller förnedrande behandling (artikel 3) kan exempelvis betraktas som kraftiga ingrepp i rätten till respekt för privatlivet, varav den kroppsliga och själsliga integriteten utgör en viktig del. Ett frihetsberövande (artikel 5) inkräktar också onekligen på privatlivet, och friheten att utöva sin religion (artikel 9) och att uttrycka sina åsikter (artikel 10) berör även de viktiga delar av privatlivet. Dessa särskilt reglerade rättigheter måste betraktas

som lex specialis inom sina respektive områden. Artikel 8 fångar därmed i första hand upp de aspekter av privatlivet som faller utanför övriga bestämmelser i konventionen. (Se Hans Danelius m.fl., Mänskliga rättigheter i europeisk praxis, Norstedts, JUNO version 6, 2023, s. 441 f.)

I första hand innebär artikel 8 en negativ förpliktelse för staten att avhålla sig från ingrepp i enskildas privatliv. Därutöver ålägger artikeln även en positiv skyldighet för staten att vidta åtgärder för att skydda den enskildes privata sfär (se t.ex. Europadomstolens avgöranden *X and Y v. the Netherlands, 26 March 1985, Series A no. 91* och *Söderman v. Sweden [GC], no. 5786/08, ECHR 2013*).

Rätten till privatliv enligt artikel 8 är mångfacetterad och omfattar ett skydd mot en mängd åtgärder och företeelser. På ett övergripande plan innebär skyddet att varje person ska ha rätt att utvecklas i förhållande till andra människor utan inblandning från utomstående. Rätten till personlig utveckling utan yttre inblandning inbegriper också en allmän rätt att bli lämnad i fred, alltså ett skydd mot alltför närgången uppmärksamhet. Detta kan innefatta ett skydd mot att bli fotograferad eller avlyssnad och att få fotografier, filmer eller ljudinspelningar av privat karaktär publicerade eller utnyttjade för ovidkommande syften. (Se Danelius m.fl., JUNO version 6, 2023, s. 460, se också t.ex. Europadomstolens avgörande *Von Hannover v. Germany, no. 59320/00, ECHR 2004-VI.*) Även registrering eller liknande behandling av personuppgifter kan omfattas av rätten till skydd för privatlivet. Enligt Europadomstolen gäller det särskilt om det i de uppgifter som registreras ingår känsliga personuppgifter, t.ex. information om politisk uppfattning, religionstillhörighet, sexuell läggning, sjukdomar, tidigare brottslighet, missbruk av droger eller liknande förhållanden (se bl.a. Europadomstolens avgörande *Segerstedt-Wiberg and Others v. Sweden, no. 62332/00, ECHR 2006-VII*, se även Danelius m.fl., JUNO version 6, 2023, s 472).

Det kan emellertid finnas legitima intressen som står emot intresset av integritetsskydd, t.ex. intresset av att använda material i brottsutredningar. I fråga om alla ingripanden i privatlivet måste det finnas en ordning som garanterar en rimlig avvägning mellan de kolliderande intressena. Det skydd för privatlivet som tillförsäkras den enskilde i artikel 8 är alltså inte absolut, utan får inskränkas i lag. Europadomstolen har i flera fall uttalat att en rimlig avvägning måste

göras mellan de kolliderande allmänna och enskilda intressen som är för handen när det gäller åtgärder som inskränker rätten till privatlivet (se bl.a. Europadomstolens avgöranden *McGinley and Egan v. the United Kingdom (revision)*, *nos. 21825/93 and 23414/94, ECHR 2000-I*, *Godelli v. Italy*, *no. 33783/09*, *25 September 2012*, *Odièvre v. France [GC]*, *no. 42326/98*, *ECHR 2003-III*, *Aycaguer v. France*, *no. 8806/12*, *22 June 2017* och det ovan nämnda *Von Hannover v. Germany*, *no. 59320/00*, *ECHR 2004-VI*, se också Danelius m.fl., JUNO version 6, 2023, s 460).

En inskränkning av rätten till privatliv måste ha stöd i lag och vara ägnat att tillgodose något av de intressen som anges i artikel 8.2, vilka bl.a. är att trygga säkerheten, förebygga brott eller med hänsyn till andra personers fri- och rättigheter. Inskränkningen ska vara nödvändig, vilket innebär att det ska finnas ett angeläget samhälleligt behov av åtgärden. Inskränkningen måste även vara proportionerlig (se Danelius m.fl., JUNO version 6, 2023, s. 443).

Om en konventionsreglerad rättighet inskränks måste den enskilde tillförsäkras vissa grundläggande rättssäkerhetsgarantier, t.ex. en rättvis rättegång och ett effektivt rättsmedel (jfr artikel 6 i konventionen). Europadomstolen har uttalat att behovet av sådana garantier är större när det gäller automatisk behandling av personuppgifter, inte minst om uppgifterna används för polisiära ändamål. Det innebär att det i nationell rätt måste säkerställas att uppgifterna är relevanta och inte för långtgående i förhållande till det ändamål för vilket de bevaras, men också att uppgifterna inte sparas under en tid som överstiger vad som är nödvändigt med hänsyn till ändamålet. Det måste också finnas garantier för att personuppgifterna skyddas från felaktig behandling. Detta gäller inte minst vid behandling av känsliga personuppgifter (se bl.a. Europadomstolens avgörande *S. and Marper v. the United Kingdom [GC]*, *nos. 30562/04 and 30566/04*, *ECHR 2008*).

3.2.3 EU:s rättighetsstadga

EU:s stadga om de grundläggande rättigheterna (rättighetsstadgan) trädde i kraft med Lissabonfördraget den 1 december 2009. Rättighetsstadgan garanterar den som är EU-medborgare vissa fri- och rättigheter och är direkt juridiskt bindande i varje EU-land.

Rättighetsstadgan har, inom ramen för fördragens tillämpningsområde, företräde framför föreskrifter i de nationella rättsordningarna. Rättighetsstadgan är emellertid endast bindande för medlemsstaternas organ och myndigheter när de tillämpar unionsrätten.

Artikel 1 i rättighetsstadgan slår fast att människans värdighet är okränkbar. Enligt artikel 3 är var och en tillförsäkrad rätt till fysisk och mental integritet. I artikel 7 tillförsäkras var och en rätt till respekt för sitt privat- och familjeliv, sin bostad och sina kommunikationer. Artikel 8 föreskriver att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Sådana personuppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. I artikel 52 anges i vilken utsträckning stadgan tillåter inskränkningar i de rättigheter som erkänns i stadgan. Av artikeln framgår att varje begränsning ska vara föreskriven i lag och förenlig med det väsentliga innehållet i rättigheterna.

Av EU-domstolens praxis kan utläsas bl.a. att en begränsning av en rättighet som sker utan hänsynstaganden till en persons individuella beteende eller omständigheter som utgångspunkt inte ska anses förenlig med det väsentliga innehållet i rättigheten (se EU-domstolens *dom av den 15 februari 2016, J. N. v Staatssecretaris van Veiligheid en Justitie, C-601/15, EU:C:2016:84*).

Vidare får begränsningar, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och svarar mot ett allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors fri- och rättigheter.

Av EU-domstolens praxis framgår att detta bl.a. innebär att åtgärder som begränsar rättigheter ska vara ägnade att uppnå de legitima mål som eftersträvas med åtgärderna i fråga, och får inte gå utöver vad som är lämpligt och nödvändigt för att uppnå dessa mål. Ett mål av allmänt samhällsintresse kan inte, oavsett hur betydelsefullt det är, i sig ensamt motivera en begränsning av en grundläggande rättighet (EU-domstolens *dom av den 8 april 2014, Digital Rights Ireland Ltd v Ireland, C-293/12, EU:C:2014:238*).

Enligt artiklarna 52.3 och 53 i rättighetsstadgan ska de rättigheter som omfattas av stadgan ges samma innebörd och räckvidd som

motsvarande rättigheter i Europakonventionen, i den mån sådana motsvarigheter finns. Detta hindrar dock inte att unionsrätten tillförsäkra ett mer långtgående skydd för grundläggande fri- och rättigheter än vad som följer av Europakonventionen.

3.2.4 Förenta nationernas (FN:s) allmänna förklaring om de mänskliga rättigheterna

FN:s allmänna förklaring om de mänskliga rättigheterna antogs år 1948. De rättigheter som omfattas av förklaringen har senare förts in och vidareutvecklats i ett antal konventioner som är bindande för de anslutna staterna. Som exempel kan nämnas 1966 års konvention om medborgerliga och politiska rättigheter. Sverige har anslutit sig till de centrala konventionerna om mänskliga rättigheter allt eftersom de har kommit till.

FN:s allmänna förklaring innehåller bl.a. bestämmelser om skydd för den personliga integriteten. I artikel 12 anges att ingen får utsättas för godtyckligt ingripande i fråga om privatliv, familj, hem eller korrespondens och inte heller för angrepp på sin heder eller sitt anseende. Vidare anges att var och en har rätt till lagens skydd mot sådana ingripanden och angrepp. I artikel 29 punkten 2 föreskrivs att inskränkningar i rättigheter och friheter endast får göras genom lag och enbart i syfte att trygga tillbörlig hänsyn till och respekt för andras rättigheter och friheter samt för att tillgodose ett demokratiskt samhälles berättigade krav på moral, allmän ordning och allmän välfärd.

En likalydande bestämmelse återfinns i artikel 17 i FN:s konvention om medborgerliga och politiska rättigheter, som antogs år 1966 och trädde i kraft år 1976.

3.2.5 Dataskyddskonventionen och Organisation for Economic Co-operation and Developments (OECD:s) riktlinjer

Europarådets ministerkommitté antog år 1981 en konvention till skydd för enskilda vid automatisk databehandling av personuppgifter (dataskyddskonventionen). Konventionen trädde i kraft den 1 oktober 1985 och syftar till att skydda den rätt till privatliv

som erkänns i artikel 8 i Europakonventionen (jfr artikel 1). I dag har 55 stater ratificerat konventionen, däribland samtliga EU:s medlemsstater.

Dataskyddskonventionens tillämpningsområde är enligt huvudregeln i artikel 3 automatiserade personregister och automatisk databehandling av personuppgifter i allmän och enskild verksamhet. Enligt artikel 4 krävs att parterna vidtar nödvändiga åtgärder i sin nationella lagstiftning för att genomföra de grundläggande principer för dataskydd som anges i konventionens andra kapitel. Dataskyddskonventionen kompletteras av ett antal av ministerkommittén antagna rekommendationer om hur personuppgifter bör behandlas inom olika områden.

År 2018 antog ministerkommittén ett ändringsprotokoll till dataskyddskonventionen. Ändringsprotokollet träder i kraft när minst 38 parter har ratificerat protokollet. Till dags dato har 31 parter ratificerat protokollet. Sverige har inte ratificerat protokollet. Sverige undertecknade protokollet den 10 oktober 2018. Syftet med ändringsprotokollet är att uppdatera konventionen och hantera de utmaningar som den tekniska utvecklingen och globaliseringen av information innebär när det gäller skyddet av privat information. Den uppdaterade konventionen kommer att ha ett enhetligt tillämpningsområde för alla konventionsparter och det kommer inte att vara möjligt att helt undanta sektorer eller verksamheter från dess tillämpning (t.ex. med hänvisning till den nationella säkerheten). Den kommer därmed att omfatta all typ av databehandling under parternas jurisdiktion inom både den offentliga och den privata sektorn.

Parallellt med dataskyddskonventionen utarbetade OECD, som är en internationell organisation med 38 EU-medlemsländer, riktlinjer för integritetsskydd och gränsöverskridande flöden av personuppgifter. Riktlinjerna uppdaterades senast år 2013. I artikel 7 i OECD:s riktlinjer anges att ”insamlingen av personuppgifter ska begränsas och att sådana bör erhållas på ett lagenligt och rättvist sätt och när det är lämpligt med den registrerades samtycke”. Dataskyddskonventionen och OECD:s riktlinjer var de viktigaste inspirationskällorna vid utformningen av EU:s regelverk för dataskydd, med början i 1995 års dataskyddsdirektiv (Europaparlamentets och rådets direktiv [95/46/EG] av den 24 oktober 1995 om skydd för enskilda personer med avseende på

behandling av personuppgifter och om det fria flödet av sådana uppgifter).

3.2.6 Barnkonventionen

FN:s konvention om barnets rättigheter (barnkonventionen) antogs av FN:s generalförsamling år 1989. Sverige ratificerade barnkonventionen år 1990 och sedan år 2020 gäller den som svensk lag (lagen [2018:1197] om Förenta nationernas konvention om barnets rättigheter). Att barnkonventionen är svensk lag innebär att domstolar och andra rättstillämpare ska beakta de rättigheter som följer av konventionen vid avvägningar och bedömningar som görs i beslutsprocesser i mål och ärenden som rör barn. Fortsatt medför även den omständigheten att Sverige som stat har ratificerat barnkonventionen, och gentemot andra stater och internationella organisationer som har åtagit sig att följa denna, att den svenska lagstiftaren har en skyldighet att se till att den nationella rätten stämmer överens med konventionen (prop. 2017/18:186 s. 60).

Konventionen vilar på, och syftar till att få genomslag för, följande grundläggande principer: (i) alla barn har samma rättigheter och lika värde, (ii) barnets bästa ska beaktas vid alla beslut som rör barn, (iii) alla barn har rätt till liv och utveckling och (iv) alla barn har rätt att uttrycka sin mening och få den respekterad.

I konventionens artikel 16 stadgas att inget barn får utsättas för godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv, sitt hem eller sin korrespondens och inte heller för olagliga angrepp på sin heder och sitt anseende. Vidare har barnet enligt samma artikel rätt till lagens skydd mot sådana ingripanden eller angrepp. Av artikel 40 följer även att barn som misstänks eller åtalas för eller som befunnits skyldigt till att ha begått brott ska behandlas på ett sätt som främjar barnets känsla av värdighet och värde. Av artikeln framgår också att barnets privatliv ska respekteras till fullo under alla stadier i förfarandet.

3.3 Begreppet personlig integritet

Det finns ingen legaldefinition av begreppet personlig integritet, vare sig i svensk grundlag, i vanlig lag eller i någon EU-rättsakt. I

Sverige blev frågan om personlig integritet föremål för rättsvetenskaplig diskussion och överväganden av lagstiftaren först under 1960-talet. 1969 års *Offentlighets- och sekretesslagstiftningskommitté* (OSK) samt 1966 års *Integritetsskyddskommitté* ansåg att grundtanken med personlig integritet kunde uttryckas på det sättet att den enskilde kan göra anspråk på en fredad privat sektor inom vilken denne kan avvisa inblandning från utomstående som uppfattas som otillbörlig (SOU 1972:47 s. 56 och SOU 1974:85 s. 56).

I stället för att försöka hitta en generell definition av begreppet personlig integritet kan betydelsen av den ringas in genom att räkna upp alla mer eller mindre olikartade enskilda situationer som kan sägas kränka den personliga integriteten. Stig Strömholm har upprättat en katalog av olika möjliga typer av kränkningar av den personliga integriteten. Dessa är följande:

- tillträde till och genomsökande av privata lokaler eller annan egendom;
- kroppsundersökning;
- medicinska undersökningar, psykologiska tester osv.;
- intrång i en persons privata sfär genom skuggning, spionerande, telefonterror och liknande;
- som ett särfall till strecksats 1 och 4: ofredande genom företrädare för massmedia;
- olovlig ljudupptagning, fotografering eller filmupptagning;
- brytande av brevhemligheten;
- telefonavlyssning;
- utnyttjande av elektronisk avlyssningsapparatur;
- spridning av förtrolig information (t.ex. genom advokater, läkare, själasörjare och liknande);
- avslöjande inför offentligheten av annans privata förhållanden;
- olika former av nyttjande av annans namn, bild eller liknande identifieringsmedel;

- missbruk av annans ord eller meddelanden (t.ex. genom förvrängda eller uppdiktade intervjuer);
- angrepp på annans heder och ära.

Dessa kränkningar kan i sin tur delas in i tre övergripande huvudgrupper: intrång, i fysisk eller annan mening, i en persons privata sfär; insamlande av uppgifter om en persons privata förhållanden; offentliggörande eller annat utnyttjande av material om en persons privata förhållanden (Stig Strömholm, ”Integritetsskyddet – ett försök till internationell lägesbestämning”, SvJT 1971, s. 695).

1984 års *Tvångsmedelskommitté* försökte, med utgångspunkt bl.a. i de vid tidpunkten gällande fri- och rättigheterna i 2 kap. RF, ringa in begreppet personlig integritet genom att skilja mellan den rumsliga integriteten (hemfriden), den materiella integriteten (egendomsskyddet), den kroppsliga integriteten (skydd för liv och hälsa, mot ingrepp i eller mot kroppen), den personliga integriteten i fysisk mening (skyddet för den personliga friheten och rörelsefriheten) och den personliga integriteten i ideell mening (skyddet för privatlivet och för personligheten inklusive den privata ekonomin). Den typ av personlig integritet som till stor del regleras genom den dataskyddsrättsliga regleringen, och som närmast är aktuell i denna utredning, är framför allt den personliga integriteten i ideell mening. (Se SOU 1984:54 s. 42.)

Uppfattningen om vad som omfattas av den personliga integriteten varierar mellan olika människor. Det beror i hög grad på den enskildes subjektiva uppfattning om vad denne anser ingå i den rent personliga sfären. Dessutom förändras inställningen till integritet över tiden. Värderingar påverkas mycket av den tidsålder och det samhälle man lever i. När det gäller uppgifter som är personliga kan det också ha betydelse i vilket sammanhang de används om den enskilde uppfattar det som att hans eller hennes integritet har kränkts eller inte. (Se prop. 2005/06:173 s. 14 f.)

Vilken reglering och begränsning av användningen av personuppgifter som är nödvändig för att skydda den personliga integriteten kan sägas till stora delar vara en fråga som är beroende av rådande värderingar i samhället. Värderingarna i samhället påverkas i sin tur bl.a. av hur informationstekniken uppfattas och används. (Se a. prop. s. 15.)

Att innebörden av personlig integritet är något som är föränderligt över tid och rum har även framhållits av OSK och 1966 års *Integritetsskyddskommitté.* OSK uttryckte detta på följande sätt. ”Svårigheterna att fastställa vad man menar med integritet sammanhänger med att en rätt att bli lämnad i fred aldrig kan vara absolut i ett samhälle. Gemenskapens krav på insatser från den enskilde i fråga om t.ex. arbete och skatter och på upplysningar erforderliga för gemensamma åtgärder måste begränsa den privata sektorn” (se SOU 1972:47 s. 56). Integritetsskyddskommittén beskrev frågeställningen på följande sätt. ”I länder med olika levnadsförhållanden och rättstraditioner sker bedömningen olika. Men uppfattningarna kan också gå isär inom ett land. Likaså förändras värderingarna med tiden. Därtill bör läggas att en individ som lever i ett samhälle och sålunda ingår i en gemenskap med andra människor inte kan göra gällande något absolut anspråk på att få leva i fred för andra individer eller ostörd av samhällets organ. Eftersom gemenskapen med andra människor och samhörigheten med samhället är grundläggande för den enskilda människans villkor, är det tydligt att tanken på skydd för dylika anspråk står i motsats till åtskilligt som av andra skäl måste gälla. Regler som syftar till att skydda den enskildes personliga integritet måste sålunda förses med olika, i skilda situationer, mer eller mindre vittgående undantag eller på annat sätt begränsas till sin giltighet, så att andra människors och samhällets intressen i övrigt inte träds för när” (se SOU 1974:85 s. 56).

Trots att det inte finns någon entydig definition av begreppet personlig integritet kan det sägas att en kränkning av densamma innebär ett intrång i en fredad sfär som den enskilde bör vara tillförsäkrad och där ett oönskat intrång bör kunna avvisas. (Se prop. 2009/10:80 s 175.)

Rätten till personlig integritet kan beskrivas som en "prima facie-rättighet". Den är en giltig och välgrundad rättighet som dock i en konkret handlingssituation kan sättas ur spel om den kommer i konflikt med någon annan rättighet som väger tyngre. (Se prop. 2005/06:173 s 16.)

Styrkan av respektive motstående rättighet kan variera med samhällsutvecklingen och framför allt med den tekniska utvecklingen. Å ena sidan kan riskerna för allvarliga kränkningar av den personliga integriteten öka genom t.ex. nya metoder att

övervaka personer och sammanställa information på. Å andra sidan kan den tekniska utvecklingen möjliggöra nya och mer effektiva sätt att exempelvis bekämpa grov brottslighet. Intresset att värna medborgarnas rättstrygghet och skydda mot de kränkningar av den personliga integriteten och andra rättigheter som det kan innebära att utsättas för brott kan då väga upp den relativt sett mindre förlust av personlig integritet som den tekniska utvecklingen kan medföra.

I detta sammanhang kan det framhållas att det allmännas skyldighet att respektera mänskliga rättigheter, t.ex. enligt Europakonvention, även innefattar positiva skyldigheter att se till att enskilda tillförsäkras skydd för sina rättigheter gentemot andra enskilda. Det innebär att staten behöver säkerställa att brott kan utredas effektivt. (Jfr prop. 2022/23:106 s. 13 och prop. 2022/23:126 s. 64.)

Det underliggande intresse som skyddet för den personliga integriteten ska tjäna har beskrivits på skiftande sätt. Det har bl.a. framhållits att tanken på att uppgifter om ens privata angelägenheter samlas in och kan komma att användas för olika ändamål kan framkalla allvarlig oro hos den enskilde, det vill säga påverka människors psykiska välbefinnande. Det kan också uppfattas som en kränkning i sig att en utomstående förfogar över uppgifter om ens privata förhållanden (SOU 1974:85 s. 57). När det specifikt gäller frågan om skydd för den personliga integriteten genom dataskydd och andra regler för personuppgiftsbehandling har den enskildes anspråk på att bli bedömd efter relevanta kriterier identifierats som ett underliggande intresse. Om man vet att en myndighet eller en organisation har tillgång till omfattande information om ens personliga förhållanden ligger det nära till hands att misstänka att informationen utnyttjas för ställningstaganden som den inte är ägnad för (SOU 1972:47 s. 57). Det är således angeläget att åtgärder som vid var tid kan anses utgöra en kränkning av den personliga integriteten också omgärdas av ett adekvat regelverk.

4 Internationell utblick

4.1 Inledning

I detta avsnitt redogörs för förekomsten och användningen av automatisk avläsning av fordons registreringsskyltar (ANPR-teknik) och ansiktsigenkänning liksom polisens möjlighet till tillgång till material från annans kamerabevakning i några relevanta europeiska länder. Aktuella uppgifter har inhämtats från Finland, Norge, Danmark, Tyskland, Nederländerna, Storbritannien, Italien och Belgien.

4.2 Användning av ANPR-teknik

4.2.1 Finland

I Finland är kameror utrustade med teknik för ANPR monterade i polisens fordon. I varje polisbil som är utrustad med ANPR-teknik finns flera videokameror, varav en är framåtriktad, en är bakåtriktad och en läser omgivande fordons registreringsskyltar. Registreringsskyltar på mötande eller omgivande fordon skannas och fordonets status vad gäller kontrollbesiktning, betalda skatter och försäkringar kontrolleras automatiskt.

Obearbetat material från den kamerabevakning med ANPR-teknik som sker med kamerorna i polisen fordon förblir lokalt lagrade (i fordonets system) i 24 timmar, varefter uppgifterna automatiskt raderas. Redigerade videor kan skickas till polisens system för användning i brottsutredningar.

Utöver ANPR-teknik har polisbilar en gruppvideoservice i form av ett system som kallas LIVE. Videokopplingen är i realtid och kan endast användas av de polismän som framför polisfordonet med kameran. Livevideoströmmen, som alltså strömmas till andra

polisenheter, kan endast sparas om uppgiften kräver det. För att kunna spara materialet från videoströmmen ska polisen kunna motivera behovet av det.

Allt inspelat material lämnar automatiskt servern efter två veckor. Användaren kan inte radera det från servern själv. För att titta på materialet krävs alltid en motivering av åtgärden.

Den lagstiftning som styr polisens användning av ANPR-teknik i denna del är 15 § lagen om behandling av personuppgifter i polisens verksamhet (616/2019; polisens personuppgiftslag) och dataskyddsdirektivet. I 15 § första stycket polisens personuppgiftslag föreskrivs att polisen får behandla uppgifter som hör till särskilda kategorier av personuppgifter endast om det är nödvändigt för ändamålet med behandlingen.

4.2.2 Norge

I Norge är kameror utrustade med ANPR-teknik installerade i cirka 70 polisfordon. Kamerorna används som indikationsverktyg för trafikkontroll och vid större evenemang. De används alltså inte regelmässigt för brottsbekämpande ändamål. Data från kamerorna lagras i 24 timmar.

Norska tullverket (*Tollvesenet*) och norska vägverket (*Statens vegvesen*) har både stationära och mobila kameror med ANPR-teknik för icke-brottsbekämpande ändamål.

4.2.3 Danmark

Den danska polisens användning regleras i föreskrift nr. 1080 av den 20 september 2017 om polisens användning av automatisk registreringsskyltsigenkänning med senare ändringar (ANPR-föreskriften). ANPR är ett internt arbetsverktyg för polisen, och behandling av personuppgifter genom ANPR får endast ske enligt reglerna i ANPR-föreskriften och endast när det är nödvändigt i samband med utförandet av polisiära uppgifter (1 § andra stycket ANPR-föreskriften).

Polisen får, enligt 4 § ANPR-föreskriften, behandla uppgifter om fordon vilka omfattas av en eller flera av de kategorier som listas i 5 §. Det kan exempelvis handla om registreringsskyltar som ska

återkallas på grund av bristande besiktning eller obetald försäkring, registreringsskyltar som är kopplade till fordon som är avregistrerade eller av andra skäl inte får användas i trafik, registreringsskyltar som är relaterade till efterlysta fordon eller som är relaterade till utredningar där en person är misstänkt för brott som kan leda till minst ett år och sex månaders fängelse.

I 5 § ANPR-föreskriften listas uttömmande de kategorier för vilka polisen har befogenhet att i förväg registrera registreringsskylten i ANPR-systemet.

Därutöver får polisen enligt 4 § ANPR-föreskriften även behandla uppgifter om fordon som inte hör till de kategorier som räknas upp i 5 §. Sådan behandling är nödvändig för att kunna hitta de fordon som omfattas av de uppräknade kategorierna, eftersom alla fordon som passerar en kamera som är utrustad med ANPR-teknik måste fotograferas av kameran. För uppgifter om fordon och registreringsskyltar som inte ger någon träff i systemet gäller dock en kortare raderingsfrist än för sådana uppgifter som ger en träff i systemet.

Det följer bl.a. av 4 § sjätte stycket lagen om brottsbekämpande myndigheters behandling av personuppgifter *(lov nr 410 af 27/04/2017 om retshåndhævende myndigheders behandling af personoplysninger; retshåndhævelsesloven*) att personuppgifter inte får lagras under längre tid än vad som är nödvändigt med hänsyn till de ändamål för vilka uppgifterna behandlas. Denna bestämmelse genomför artikel 4.1 e dataskyddsdirektivet. Vid fastställande av raderingsfrister måste således en bedömning göras av nödvändigheten och proportionaliteten av att lagra personuppgifterna. Bedömningen inkluderar å ena sidan hänsyn till polisens operativa och utredningsmässiga behov av att uppgifterna lagras, och å andra sidan den registrerades rättigheter.

När det gäller sådana uppgifter som har gett en träff i systemet ska, enligt 6 § första stycket ANPR-föreskriften, uppgifter om registreringsskyltar som omfattas av en eller flera av de kategorier som listas i 5 § ANPR-föreskriften raderas senast tre månader, ett år eller två år efter insamlingen, beroende på vilken kategori uppgifterna omfattas av.

Vad gäller uppgifter som inte har gett träff i systemet kan information om registreringsskyltar som inte omfattas av uppräkningen i 5 § ANPR-föreskriften behandlas dels när

informationen samlats in med hjälp av stationär ANPR-utrustning och insamlingen har skett inom ramen för en eller flera strategiska insatsområden inom polisen där användningen av ANPR bedöms vara av väsentlig betydelse, dels när informationen samlats in med hjälp av mobil ANPR-utrustning som en del av en riktad polisiär insats, och insatsen är tidsmässigt och geografiskt begränsad och genomförd baserat på en konkret polisiär bedömning där användningen av ANPR har bedömts vara av väsentlig betydelse för insatsen.

Slutligen kan, enligt 6 § andra stycket ANPR-föreskriften, uppgifter som samlats in med hjälp av mobil ANPR-utrustning behandlas under en kortvarig period, även om den inte samlats in som en del av en riktad polisiär insats. Personuppgifter som inte gett träff i systemet ska raderas 60 dagar efter det att de samlats in. Uppgifter som samlats in med mobil ANPR-utrustning ska dock raderas redan efter sju dagar om den inte samlats in som en del av en riktad polisiär insats.

De nuvarande raderingsreglerna i ANPR-föreskriften ändrades senast år 2022, då raderingsfristerna för icke-träffar förlängdes från 30 dagar till 60 dagar för uppgifter från annan ANPR-bevakning än sådan som sker med mobil ANPR-utrustning, och från 24 timmar till sju dagar för sådana uppgifter som inhämtats genom mobil ANPR-bevakning. Detta skedde bl.a. med hänsyn till det bedömda höga operativa värdet av ANPR-informationen för polisens insatser mot bl.a. gränsöverskridande brottslighet. Ändringarna gjordes efter samråd med Datatilsynet och enligt det danska justitieministeriets bedömning utgjorde de en rimlig avvägning av relevanta hänsyn.

4.2.4 Tyskland

Tyskland är ett federalt organiserat land. Vart och ett av de 16 förbundsländerna har egna poliskårer och i viss utsträckning egen polislagstiftning. Denna redogörelse avser de regler som gäller för den federala tyska polisen, *Bundespolizei* (förbundspolisen).

Automatiserad registrering av fordons registreringsskyltar hos Bundespolizei får användas för två olika övergripande ändamål: avvärja faror eller bekämpa brott.

När det gäller den första av dessa två ändamål, att avvärja faror, finns den rättsliga grunden huvudsakligen i 27 b § lagen om förbundspolisen (*Bundespolizeigesetz; BPolG*). I denna bestämmelse finns regler om s.k. ”ändamålsrelaterad automatisk registrering av registreringsskyltar”. I bestämmelsen föreskrivs i huvudsak följande.

- Det är nödvändigt för att avvärja en pågående fara för en persons kropp, liv eller frihet,
- det är nödvändigt med hänsyn till faktiska indikationer om brott av väsentlig betydelse mot gränssäkerheten, eller
- en person eller ett fordon är efterlyst av Bundespolizei eller en annan myndighet och det finns en överhängande och omedelbar risk att personen kommer begå ett allvarligt brott, eller att det efterlysa fordonet kommer användas vid ett allvarligt brott.

De uppgifter som samlats in på detta sätt får automatiskt jämföras med en sökfil. Vid en träff kontrolleras omedelbart överensstämmelsen mellan de insamlade uppgifterna och uppgifterna i sök-filen. Vid en träff kan de insamlade uppgifterna bearbetas och överföras.

Om det inte sker en träff måste uppgifterna omedelbart raderas. Detsamma gäller om jämförelsen visserligen leder till en träff, men de ändamål för vilka uppgifterna förts in i sökfilen inte är relaterad till de ändamål för vilka ANPR-bevakning har skett. Detta gäller inte om uppgifterna behövs för att utreda ett allvarligt begånget brott.

När det gäller användning av ANPR-teknik i brottsbekämpande syfte regleras detta främst av 163 g § straffprocesslagen (*Strafprozessordnung; StPO*). Denna bestämmelse föreskriver i huvudsak följande.

På offentlig plats i trafiken får registreringsskyltar för motorfordon samt plats, datum, tid och färdriktning samlas in automatiskt med tekniska medel utan de berörda personernas kännedom, om det finns tillräckliga faktiska indikationer på att ett brott av betydande allvar har begåtts och det är motiverat att anta att åtgärden kan leda till att den misstänkte identifieras eller att hans vistelseort klarläggs. Denna automatiska uppgiftsinsamling måste vara tids-mässigt och geografiskt begränsad. Uppgifter får alltså inte för detta ändamål samlas in regelmässigt och med allmän geografisk täckning.

Uppgifter om registreringsskyltar för motorfordon som samlats in på detta sätt får automatiskt jämföras med registreringsskyltarna för motorfordon som är registrerade på den misstänkte eller används av honom eller som används av personer andra än den misstänkte om det, på grundval av särskilda omständigheter, kan antas att de är kopplade till den misstänkte, och det skulle innebära betydligt större svårigheter att fastställa den misstänktes vistelseort med andra medel.

Jämförelsen måste ske omedelbart efter den automatiska datainsamlingen. Vid en träff måste överensstämmelsen omedelbart kontrolleras manuellt. Om det inte finns någon träff eller den manuella kontrollen inte bekräftar träffen måste de uppgifter som samlats in raderas omedelbart.

De åtgärder som nu har nämnts kan bara vidtas efter beslut av en åklagare. Åklagaren måste visa på att förutsättningar som krävs för åtgärderna föreligger och uppge vilka uppgifter som de automatiskt insamlade uppgifterna ska jämföras med. Beslutet måste, i enlighet med vad som sagts ovan, vara begränsat tidsmässigt och geografiskt. Om det föreligger en överhängande fara får beslutet även utfärdas muntligen och av en utredare. I sådant fall måste personen som utfärdat beslutat lämna en skriftlig bekräftelse inom tre dagar.

Om förutsättningarna för beslutet inte längre är uppfyllda eller syftet med åtgärderna har uppnåtts måste åtgärderna avslutas omedelbart.

4.2.5 Nederländerna

Nederländsk polis och åklagare använder ANPR-teknik på tre olika sätt: (1) för realtidsvarning och uppföljning, (2) som ett led i brottsutredningar, samt (3) som ett led i att upprätthålla trafiklagstiftningen.

Realtidsvarning innebär att brott eller kriminellt beteende upptäcks i det ögonblick de inträffar eller när ett fordon kopplat till en efterlyst individ passerar en kamera, med avsikt att omedelbart följa upp händelsen. Sådana varningar i realtid kan utfärdas av två olika skäl, dels baserat på en referenslista, dels baserat på ett visst beteendemönster.

Att varna och följa upp baserat på en referenslista är den vanligaste användningen av ANPR-teknik. Referenslistan innehåller registreringsskyltar för fordon som av ett eller annat skäl påkallar polisens uppmärksamhet, exempelvis stulna fordon, fordon registrerade på personer som har rymt från frihetsberövande straff, fordon med obetalda böter, fordon kopplade till tidigare överträdelser av trafiklagar osv. När ett fordon på referenslistan passerar en kamera genereras en träff. Denna träff loggas, och den relevanta informationen om träffen överförs i realtid till lokala polisenheter för uppföljning och åtgärd.

När det gäller den andra situationen, realtidsvarning baserad på ett beteendemönster, finns det ingen förkunskap hos polisen om fordonet eller personens identitet. I stället är varningen enbart eller huvudsakligen baserad på ett fordons beteende, vilket är en kombination av faktorer som indikerar möjlig inblandning i ett brott. Ett exempel kan vara ett fordon som är ofta förekommande i närheten av en person som ska skyddas eller en registreringsskylts-kombination som passerar kameran nästan samtidigt vid två platser som är långt åtskilda från varandra. För dessa ändamål registreras och lagras uppgifter om alla fordonspassager förbi kameror som är utrustade med ANPR-teknik i 28 dagar. Åtkomst till uppgifterna i databasen kan endast fås efter beslut av en åklagare. För sådana åtkomstbeslut gäller vissa förutsättningar och endast vissa poliser har behörighet att få tillgång till databasen.

Därutöver är kameror med ANPR-teknik installerade i hela landet för att handha automatisk hastighetsövervakning och för att bevaka lydnad av signaler vid trafikljus. Om en sådan kamera registrerar en överträdelse utfärdas böter omedelbart och utan mänsklig inblandning

4.2.6 Storbritannien

I Storbritannien används ett gemensamt nationellt ANPR-system. Till detta system är kopplat fler än 18 000 kameror med ANPR-teknik, som varje dag i genomsnitt skickar över 80 miljoner läsningar av registreringsskyltar till det nationella systemet.

Den nationella lagstiftning som reglerar användningen av ANPR-teknik inkluderar 2018 års dataskyddslag (*Data Protection Act;*

DPA), Storbritanniens nationella allmänna dataskyddsförordning (*UK GDPR*), *Protection of Freedoms Act 2012* samt vägledningar från den nationella brittiska tillsynsmyndigheten för dataskydd Information Commissioner's Office.

ANPR-infrastrukturen får endast användas för brottsbekämpningsändamål enligt definitionen i DPA eller för ändamål hänförliga till nationell säkerhet. Brottsbekämpningsändamål definieras av DPA som "förhindrande, utredning, upptäckande eller lagförande av brott, eller verkställande av straff, inklusive skydd mot och förebyggande av hot mot allmän säkerhet".

Uppgifter från ANPR-bevakning får lagras i högst tolv månader efter den ursprungliga insamlingen av uppgifterna, om det inte därefter finns grund för att fortsätta behandla uppgifterna enligt den brittiska straffprocesslagen (*Criminal Procedure and Investigations Act 1996*), som reglerar polisens utredningsprocess och behandlingen av material som hittas eller genereras i samband med en utredning.

Inrikesdepartementet (*Home Office*) utfärdar nationella ANPR-standarder för polisarbete och brottsbekämpning (*National ANPR standards for policing and law enforcement; NASPLE*). Dessa ger den övergripande vägledningen för nationell användning av ANPR-teknik. Denna vägledning kompletteras av nationella standarder för tillsyn över användningen av ANPR-teknik. Dessa innehåller tydliga regler om begränsning och kontroll av åtkomst till lagrade ANPR-uppgifter, i syfte att säkerställa att dessa endast används för officiella utredningsändamål.

Enskilda tjänstemän har endast tillgång till sådana uppgifter om det är relevanta för deras konkreta arbetsuppgifter. De flesta tjänstemän som har behörighet att komma åt lagrade ANPR-uppgifter får bara göra det i högst 90 dagar från det att uppgifterna samlades in.

4.2.7 Italien

I Italien regleras polismyndigheternas användning av ANPR-teknik i ett flertal olika författningar. De exakta rättsliga gränserna för användningen av ANPR-teknik kan variera baserat på lokala föreskrifter, liksom lokala riktlinjer som fastställts för skyddet av integritet och personuppgifter.

Det övergripande rättsliga ramverket finns, utöver i EU:s dataskyddsförordning, dels i väglagen (*Codice della Strada, n. 285/1992*), dels i det legislativa dekretet av den 30 juni 2003 (*decreto legislativo n. 196/2003*).

I artikel 126 *bis* i den italienska väglagen stadgas att behandlingen av uppgifter som samlats in av ANPR-teknik endast är tillåten för följande ändamål.

- Att upptäcka och lagföra överträdelser av väglagen, inklusive trafikbrott.
- Att leta efter fordon som är inblandade i trafikolyckor.
- Att leta efter fordon som är efterlysta eller som berörs av en brottsutredning.
- För ändamål relaterade till allmän säkerhet.

Behandlingen av data som samlats in av ANPR-teknik måste utföras i enlighet med de grundläggande dataskyddsrättsliga principerna, bl.a. uppgiftsminimering, att behandling endast får ske för uttryckliga och specifika ändamål, samt att uppgifterna måste lagras och skyddas på ett betryggande sätt.

De italienska polismyndigheterna är vidare skyldiga att informera den nationella italienska dataskyddsmyndigheten om installationen och användningen av ANPR-system. Polismyndigheterna är även skyldiga att implementera lämpliga tekniska och organisatoriska åtgärder för att säkerställa säkerheten för de insamlade uppgifterna, särskilt för att förhindra obehörig åtkomst, eller att uppgifter förvanskas eller förstörs.

4.2.8 Belgien

Artikel 44.11.3 *septies* i den belgiska polislagen (*Wet op het Politieambt; WPA*) föreskriver att ANPR-teknik får användas för fyra olika ändamål.

Dels får ANPR-teknik användas för att underlätta utförandet av polisens lagstadgade uppgifter avseende:

- att upptäcka och lagföra förseelser och brott, inklusive att verk-ställa straff eller andra frihetsberövande åtgärder;

- att övervaka förseelser i vägtrafiken; eller
- att spåra försvunna personer, när det finns allvarliga misstankar om eller indikationer på att den försvunna personen är i omedelbar fysisk fara.

Dels får ANPR-teknik också användas för att underlätta polisens utförande av sitt uppdrag när det gäller att övervaka den allmänna ordningen i vissa situationer.

4.3 Användning av ansiktsigenkänning

4.3.1 Finland

Den finska polisen använder ett system för automatisk ansiktsigenkänning som benämns KASTU. Systemet används inte i realtid, utan endast för ansiktsigenkänning i efterhand.

Systemet har två huvudsakliga användningsområden. Det används dels inom ramen för brottsutredande verksamhet, för att jämföra en ansiktsbild mot bilder i polisens register i syfte att identifiera misstänkta. Det används dels också när enskilda ansöker om pass eller ID-handlingar, för att jämföra den gamla bilden från det tidigare passet med den nya bilden för att säkerställa att det är samma person.

De regler som gäller för användandet av ansiktsigenkänning grundar sig ytterst på dataskyddsdirektivets bestämmelser om behandlingen av särskilda kategorier av personuppgifter (artikel 10).

Enligt 6 § lagen om behandling av personuppgifter i brottmål (1054/2018) måste de personuppgifter som behandlas vara adekvata och nödvändiga med hänsyn till ändamålet med behandlingen och får inte vara för omfattande i förhållande till de ändamål för vilka de behandlas. Enligt 15 § första stycket lagen om behandling av personuppgifter i polisens verksamhet (616/2019; polisens personuppgiftslag) får polisen behandla uppgifter som hör till särskilda kategorier av personuppgifter (jfr artikel 10 i dataskyddsdirektivet) endast om det är nödvändigt för ändamålet med behandlingen. I andra stycket i samma bestämmelse föreskrivs att biometriska uppgifter som behandlas för utförande av de uppgifter som föreskrivs i lagen om identitetskort (663/2016) och

passlagen (671/2006) får användas för andra ändamål än det ursprungliga ändamålet med behandlingen av uppgifterna endast om det är nödvändigt för att identifiera ett offer för en naturkatastrof, storolycka eller någon annan katastrof eller ett offer för ett brott eller ett offer som annars förblivit oidentifierat. Rätt att använda uppgifterna har endast den som nödvändigtvis måste använda dem för skötseln av sina arbetsuppgifter. Uppgifter som tagits för jämförelse får användas endast när jämförelsen görs och ska därefter omedelbart förstöras.

Vidare föreskrivs i 2 § polisens personuppgiftslag att bl.a. proportionalitetsprincipen och principen om ändamålsbundenhet ska iakttas vid behandling av personuppgifter, vilket innebär att KASTU-systemet inte kan användas för att utreda vilket brott eller vilken förseelse som helst. Enligt polisstyrelsens riktlinjer får således KASTU-systemet endast användas för att utreda gärningar som kan utgöra brott på vilket fängelse kan följa.

Utgångspunkten vid användningen av KASTU-systemet är att det, för att användning ska vara tillåtet, ska vara nödvändigt för polisen att utreda en okänd parts identitet för undersökning och övervakning eller för att förebygga eller avslöja brott. Om den okända parten kan identifieras på annat sätt ska KASTU-systemet inte användas för identifikation.

4.3.2 Norge

Norge är inte medlem av EU, men är en del av Europeiska ekonomiska samarbetsområdet (EES) och Schengenområdet. I Norge används automatiserad ansiktsigenkänning vid ansökningar om pass, ID-kort, visum, uppehållstillstånd och automatiserad gränskontroll (eGates för EES-medborgare). Under år 2024 kommer polisen att börja använda tekniken i större utsträckning vid gränskontroll i samband med implementeringen av det s.k. Entry Exit-systemet inom EES-området.

Automatiserad ansiktsigenkänning används även i viss utsträckning av polisen inom ramen för brottsutredningar. I brottsutredningar kan polisen använda automatiserad ansiktsigenkänning på övervakningsmaterial. Detta sker endast i efterhand, på så sätt att

inspelningar behandlas med ansiktsigenkänningsteknik för att utreda brott.

Den norska polisen har inte laglig möjlighet att använda automatiserad ansiktsigenkänning i realtid.

4.3.3 Danmark

Ansiktsigenkänning används endast i mycket begränsad utsträckning i polisens brottsbekämpande verksamhet i Danmark.

De danska brottsbekämpande myndigheternas användning av ansiktsigenkänning regleras i lagen om brottsbekämpande myndigheters behandling av personuppgifter *(lov nr 410 af 27/04/2017 om retshåndhævende myndigheders behandling af personoplysninger; retshåndhævelsesloven*). Enligt denna lag är polisen inte förhindrad från att identifiera en fysisk person genom användning av t.ex. ansiktsigenkänningsteknologi, men behandlingen av känsliga personuppgifter är likväl föremål för en strikt nödvändighetsbedömning. Det framgår av 10 § andra stycket lagen att behandling av känsliga personuppgifter endast får äga rum när det är strikt nödvändigt och sker med syfte att bl.a. förebygga, utreda, avslöja eller åtala brott eller för att förebygga hot mot allmän säkerhet. Förutom denna nödvändighetsbedömning måste eventuell ansiktsigenkänningsteknologi även bedömas med avseende på andra bestämmelser i lagen. Det innebär särskilt de grundläggande principerna om bl.a. god databehandlingssed och proportionalitet, vilka framgår av 4 § i lagen.

Det finns ingen översikt över vilka danska myndigheter och privata aktörer som använder ansiktsigenkänningsteknologi.

När det gäller privata aktörers användning av ansiktsigenkänningsteknologi följer det av 7 § fjärde stycket dataskyddslagen (*databeskyttelsesloven*) att den nationella danska tillsyns-myndigheten för dataskydd (*Datatilsynet*) måste ge tillstånd om en privat registeransvarig vill behandla känsliga uppgifter, inklusive biometriska data. Sådant tillstånd ska endast ges under de förutsättningar som anges i artikel 9 andra stycket (g) dataskyddsförordningen, det vill säga Datatilsynet ska alltså underrättas och ge tillstånd för behandling av biometriska data med hjälp av ansiktsigenkänningsteknologi, om den registeransvarige är en privat

aktör och behandlingen av personuppgifter är nödvändig av hänsyn till viktiga samhällsintressen. Om den registeransvarige använder ansiktsigenkänning baserat på en annan rättslig grund än denna, t.ex. den registrerades samtycke, är det inte nödvändigt att få tillstånd från Datatilsynet. Datatilsynet har därför inte heller en fullständig översikt över vilka privata aktörer som använder ansiktsigenkänningsteknologi.

Vad gäller den praktiska användningen av ansiktsigenkänning av dansk polis har ansiktsigenkänningsteknologi tidigare använts av Köpenhamnspolisen under perioden april 2016 till hösten 2021, i samband med den automatiserade in- och utresekontrollen (s.k. ABC-eGates; Automatic Border Control) på Köpenhamns flygplats. Det har installerats nya ABC-eGates-moduler på Köpenhamns och Billunds flygplatser som för närvarande inte är i drift. Dessa moduler förväntas tas i drift i vart fall på Billunds flygplats under första kvartalet 2024.

Nationalt Cyber Crime Center (NC3), som är en enhet inom Nationella enheten för särskilda brott (NSK), har nyligen inlett ett pilotprojekt gällande användningen av ansiktsigenkänningsteknologi. Teknologin kommer under pilotprojektet att testas som ett verktyg för att söka igenom bild- och videomaterial i ett antal avslutade utredningar samt i NC3:s databas med bildmaterial relaterat till sexuellt utnyttjande av barn.

Ett av polisdistrikten i Köpenhamn (Københavns Vestegn) har sedan år 2022 i två specifika fall använt ett program som bl.a. inkluderar en funktion för ansiktsigenkänning för att lokalisera specifika barn som utsatts för övergrepp. Polisen har emellertid därefter på eget initiativ slutat använda programmet. Den danska Rigspolisen har därefter informerat att om det blir aktuellt för polisen att börja använda ansiktsigenkänningsteknologi mer systematiskt eller på annat sätt omfattande krävs en rad närmare principiella och juridiska överväganden, som kommer att äga rum med inblandning av det danska justitiedepartementet.

4.3.4 Tyskland

Programvara för automatisk ansiktsigenkänning används för närvarande inte av den federala tyska polisen (*Bundespolizei*) för något

ändamål. I det nu gällande koalitionsavtalet mellan regeringspartierna SDP, De Gröna och FDP har partierna kommit överens om den politiska viljeinriktningen att framgent avvisa omfattande användning av kamerabevakning och användningen av biometrisk registrering för övervakningsändamål.

4.3.5 Nederländerna

Den nederländska polisen använder ett system för ansiktsigenkänning som heter CATCH (*Centrale Automatische Technologie voor Herkenning*). CATCH finns i två versioner, en som används i brottsbekämpande verksamhet och en version som används för gränskontroll.

Den version av CATCH som används inom brottsbekämpningen hjälper till att identifiera en okänd persons identitet genom att generera en biometrisk profil från ansiktsfotografier som förekommer i en brottsutredning. CATCH jämför sedan denna data med biometriska profiler som lagrats i en referensdatabas, som innehåller ansiktsbilder på misstänkta och dömda individer. Jämförelsen är begränsad till den uppsättning bilder som förekommer i referensdatabasen. CATCH genererar en kandidatlista över ansikten som liknar det sökta fotot. En expert granskar detta resultat, och om experten är övertygad om att likheten är tillräcklig med en kandidat från listan presenteras matchningen för två andra experter för oberoende bedömning. Om båda dessa experter når samma slutsats som den första experten rapporteras det som ett slutligt resultat av ansiktsigenkänningen. Det finns därvid fyra möjliga resultat som kan rapporteras: att experterna ser *många likheter* mellan den biometriska profilen och referensbilden, att experterna ser *likhet*, att experterna ser *skillnader*, eller att *ingen slutsats* kan dras. Vid oenighet mellan experterna vidarerapporteras endast den mest för-siktiga av dessa fyra slutsatser. Den polisrapport som genereras på detta sätt fungerar som en utgångspunkt för vidare utredning. Ett frihetsberövande kan aldrig göras endast på grundval av en ansiktsjämförelse som har gjorts med hjälp av CATCH.

Justitie- och säkerhetsministern har i ett brev till det nederländska parlamentet uttalat att det inte är aktuellt att införa lagliga möjligheter till ansiktsigenkänning i realtid på offentlig plats.

I samma brev slog ministern fast att om polisen avser att använda ansiktsigenkänningsteknik på ett annat sätt än genom CATCH-systemet, måste polisen först genomföra en juridisk, teknisk och etisk bedömning. Den nederländska polisen har utvecklat ett ramverk för bedömning för att kunna utföra en sådan utvärdering. Hittills har godkännande för användning beviljats för en engångsanvändning av ytterligare endast ett system, FaceF1nder. Med FaceF1nder-systemet kan polisen söka efter ansikten i omfattande samlingar av foton eller videor, t.ex. för att undersöka brott som fångats av många övervakningskameror under en längre period, eller för att genomföra sökningar i alla foton och videor på exempelvis en beslagtagen smartphone.

4.3.6 Storbritannien

Den brittiska polisen använder för närvarande tre typer av ansiktsigenkänning: retrospektiv ansiktsigenkänning, det vill säga ansiktsigenkänning i efterhand (*retrospective facial recognition; RFR*), ansiktsigenkänning i realtid (*live facial recognition; LFR*) och operatörinitierad ansiktsigenkänning (*operator initiated facial recognition; OIFR*).

RFR, det vill säga ansiktsigenkänning i efterhand, används efter att en händelse eller en incident har ägt rum, exempelvis efter att ett misstänkt brott har begåtts. RFR sker alltid inom ramen för en brottsutredning. De bilder som analyseras tillhandahålls vanligtvis från övervakningskameror, mobiltelefonvideor, bevakningskameror i fordon, s.k. ”dörrklockekameror” eller från sociala medier. Dessa bilder jämförs sedan med bilder på personer tagna vid gripandet för att identifiera en misstänkt.

När RFR leder till en möjlig träff granskar en särskilt utbildad operatör samt en utredare bilderna för att bekräfta träffen. Utredaren kommer inom ramen för utredningen att, oavsett RFR-matchningen, överväga all tillgänglig bevisning och följa upp alla rimliga ledtrådar, precis som i vilken brottsutredning som helst.

Användningsområdet är huvudsakligen att identifiera misstänkta personer snabbare och mer noggrant, men RFR kan också hjälpa till att identifiera t.ex. saknade eller avlidna personer. En studie som har utförts av den brittiska polisen har funnit att identifiering utan RFR i genomsnitt tar cirka 14 dagar, medan identifiering med hjälp av RFR vanligtvis tar ett fåtal minuter.

Alla lokala och regionala brittiska poliskårer använder som jämförelsematerial vid RFR en nationell polisiär databas för ansiktssökningar.

För ansiktsigenkänning i realtid (LFR) gäller följande. Alla insatser är riktade, grundar sig på underrättelseinformation samt är geografiskt och tidsmässigt begränsade. LFR används alltså endast på de platser och vid de tider då det är troligt att insatsen kommer ha en konkret effekt. Innan en insats med LFR informerar polisen allmänheten om var man avser att använda tekniken och var allmänheten kan få mer information om vad detta innebär.

Tekniken använder livevideo av människor som passerar en kamera och jämför dessa bilder i realtid med en specifik lista över personer som är efterlysta av polisen. Tekniken kan exempelvis hitta och välja ut ett ansikte som eventuellt tillhör en efterlyst person ur en tät folkmassa. Det innebär att polisen på så sätt kan identifiera efterlysta brottslingar och gripa dem.

Efter en eventuell LFR-träff är det alltid polis på plats som beslutar vilken åtgärd, om någon, som ska vidtas. Precis som vid vilken polisutredning som helst måste det finnas skäl att misstänka att den personen som identifierats har gjort sig skyldig till ett brott och att det finns skäl för ett frihetsberövande. Standardprocedurerna för utredning, bevisinsamling, gripande och åtal följs.

När ingen träff mot bevakningslistan sker raderas en persons biometriska data omedelbart och automatiskt. Bevakningslistan förstörs efter varje enskild insats.

Det är ett operativt beslut för enskilda poliskårer om, hur och när man ska använda tekniken, i linje med etiska och yrkesmässiga riktlinjer som utfärdas av den brittiska nationella polishögskolan College of Policing. Hittills har tre brittiska lokala poliskårer beslutat sig för att använda LFR: South Wales Police (SWP), Metropolitan Police Service (MPS) och Northamptonshire Police. Metropolitan Police Service är poliskåren för Stor-London.

Vid operatörsinitierad ansiktsigenkänning (OIFR) används en mobilapplikation som låter enskilda poliser fotografera en person och kontrollera personens identitet, utan att personen behöver frihetsberövas för att därefter kunna identifieras. OIFR-applikationen är än så länge på ett tidigt teststadium men har visat positiva resultat.

4.3.7 Italien

I Italien används ansiktsigenkänning i efterhand inom ramen för de brottsbekämpande myndigheternas brottsutredande verksamhet.

De italienska brottsbekämpande myndigheterna får endast använda ansiktsigenkänningssystem för specifika och legitima ändamål, i enlighet med det europeiska dataskyddsregelverket.

I Italien används ansiktsigenkänningssystem för polisiära ändamål, i form av utredning av brott, gränskontroll och skydd av allmänna platser. Den nationella italienska tillsynsmyndigheten för dataskydd har publicerat riktlinjer om användningen av ansiktsigenkänningssystem av polismyndigheterna. Dessa riktlinjer fastslår bl.a. att ansiktsigenkänningssystem måste användas på ett transparent och ansvarsfullt sätt, och att medborgare måste informeras om användningen av dessa teknologier.

De rättsliga begränsningarna enligt italiensk rätt för användning av ansiktsigenkänning korresponderar med de begränsningar som framgår av det EU-rättsliga dataskyddsregelverket, och kan sammanfattas enligt följande.

- Ansiktsigenkänningssystem får endast användas för specifika ändamål, såsom förebyggande och upptäckt av brott, sökandet efter försvunna personer eller skydd av allmän säkerhet.
- Ansiktsigenkänningssystem får bara användas när det är nödvändigt och proportionerligt. Otillbörligt ingripande i medborgarnas rättigheter och friheter måste undvikas.
- Data som samlats in genom ansiktsigenkänningssystem får endast lagras under den tid som är nödvändig för att uppnå det syfte för vilket de samlades in.

- Data som samlats in genom ansiktsigenkänningssystem måste skyddas från obehörig åtkomst, liksom från att ändras eller förstöras.

De italienska polismyndigheterna är skyldiga att informera den nationella italienska tillsynsmyndigheten för dataskydd om installationen och användningen av ansiktsigenkänningssystem.

Användningen av ett system för ansiktsigenkänning i realtid (det så kallade SARI-systemet) blev avstyrkt av den italienska nationella tillsynsmyndigheten för dataskydd, och har följaktligen inte driftsatts. Den italienska polisen har inte i dag tillgång till system för ansiktsigenkänning i realtid.

4.3.8 Belgien

Ansiktsigenkänning används inte för identifiering i realtid i Belgien. De belgiska brottsbekämpande myndigheterna har endast möjlighet att använda ansiktsigenkänning i efterhand, inom ramen för en brottsutredning. Användning av ansiktsigenkänningsteknik sker i sådana situationer under kontroll av åklagare och endast i syfte att verifiera identiteten hos en utpekad misstänkt person.

4.4 Polisens tillgång till material från annans kamerabevakning

4.4.1 Finland

Den finska polisen har tillgång till en digital miljö som innehåller verktyg för att samla in och bearbeta bevakningsvideomaterial från polisen, andra myndigheter, privata operatörer eller kommuner. Materialet kan samlas in direkt från andra operatörer (om överenskommelser om detta finns) eller begäras från dem.

Materialet lagras i en mapp som är ansluten till ett undersökningsärende där auktorisationer flödar nedåt och metadata automatiskt infogas i materialet.

4.4.2 Norge

Den norska polisen har sina egna kameror för bevakning av centrala platser i Oslos centrum med direkt tillgång i realtid. Polisen har också sina egna kameror för bevakning av Brummundals centrum, men dessa används endast för inspelning. Dessa inspelningar sparas i sju dagar.

Den norska polisen har inte automatisk tillgång till bevakningskameror som ägs av andra offentliga organ.

Tillgång till inspelningar från privat, kommunal eller statlig kamerabevakning kan erhållas på frivillig väg utan en formenlig rättslig begäran om överlämning till den ansvariga för behandlingen av kamerabevakningen. Detta är möjligt på grund av undantagen i personuppgiftslagen (*lov 15 juni 2018 nr 38 om behandling av personopplysninger*) som tillåter sådan överlämning till polisen. Det finns etablerade kontaktpunkter och rutiner för att hämta inspelningar från kameror från större aktörer där det sker frekvent, t.ex. material från kameror på offentliga transportmedel.

Den norska polisen har under vissa förutsättningar befogenhet att använda kamerabevakning från drönare. Polisen har även möjlighet att, efter beslut härom, bedriva dold kamerabevakning på offentliga och privata platser.

4.4.3 Danmark

Någon information finns inte tillgänglig.

4.4.4 Tyskland

För närvarande har den federala tyska polisen Bundespolizei ingen direkt åtkomst till kamerabevakningsmaterial från andra myndigheter.

Inom ramen för järnvägspolisens (*Bahnpolizei*) uppgifter är direkt åtkomst till uppgifter från kamerabevakning som bedrivs av Deutsche Bahn möjlig.

När det gäller platser som flygplatser eller gränsområden har Bundespolizei eller gränspolisen (*Grenzschutz)* i allmänhet egna kamerainstallationer. Bundespolizei och gränspolisen har i regel

även egna kamerainstallationer på privata flygplatser. När det finns behov av det inom ramen för den brottsbekämpande verksamhet, eller i syfte att avvärja faror, kan polisen i vissa fall få tillgång till bildströmmar i realtid från dessa polisiära bevakningskameror på tågstationer och flygplatser. Detta är dock beroende av om den kamerainstallationen rent tekniskt stöder sådan överföring i realtid, vilket inte är fallet med alla kamerainstallationer.

Om uppgifter från kamerabevakning som bedrivs av andra myndigheter är relevanta som bevis inom ramen för Bundespolizeis brottsbekämpande verksamhet kan uppgifterna säkras, bl.a. genom bevisbeslag enligt 94 § straffprocesslagen (*Strafprozessordnung; StPO*). Enligt 98 § StPO kan sådant beslag endast beslutas av en domstol eller, vid fara i dröjsmål, av åklagare eller av en utredare som arbetar för en åklagare.

De lagliga kraven för att Bundespolizei i sin tur ska kunna föra över personuppgifter (t.ex. material från kamerabevakning) till andra brottsbekämpande myndigheter framgår av 32 § punkterna 1 och 2 i den tyska polislagen (*Bundespolizeigesetz; BPolG*). Där framgår att Bundespolizei kan överföra person-uppgifter till andra brottsbekämpande myndigheter samt i vissa fall till tullmyndigheter i den utsträckning det är nödvändigt för dessa myndigheter att utföra brottsbekämpande uppgifter. Detta gäller även för överföring av personuppgifter mellan olika organisations-enheter inom Bundespolizei.

Det framgår vidare att Bundespolizei kan överföra person-uppgifter till andra inhemska offentliga organ i den utsträckning det är nödvändigt bl.a. för att

- utföra en uppgift som åligger dessa organ,
- avvärja faror,
- avvärja allvarlig kränkning av enskilda rättigheter, eller
- utreda brott eller lagöverträdelser samt verkställa straff.

Genom 32 a § i BPolG skapas förutsättningarna för överföring av personuppgifter till brottsbekämpande myndigheter i andra medlemsstater i EU.

4.4.5 Nederländerna

För kameror som ägs av kommuner är chefsåklagaren den lagliga dataskyddsansvarige. Polisen har tillgång material från sådana kameror, om det behövs för utredningsändamål.

Kamerabilder från andra organisationer eller privatpersoner kan rekvireras av polisen, och kameraägaren är skyldig att tillhandahålla bilderna. Det är därvid åklagaren, som i Nederländerna är förundersökningsledare, som själv kan besluta om att begära in sådant material, eller att belägga det med bevisbeslag.

4.4.6 Storbritannien

Bevakningskameror ägs dels av de lokala och nationella polismyndigheterna, dels av myndigheter på kommunal nivå, dels av privata företag. I grund och botten hanterar och använder var och en sina egna system.

Det finns ingen nationell lagstiftning som specifikt reglerar frågan om polisens tillgång till material från annans kamerabevakning. Den brittiska nationella tillsynsmyndigheten för dataskydd, Information Commissioner's Office, har dock publicerat en vägledning för att hjälpa organisationer inom både den offentliga och privata sektorn som använder kamerabevakningssystem när det gäller behandlingen av personuppgifter. Syftet är att hjälpa organisationer att hålla sig inom de lagliga ramarna i Storbritanniens nationella allmänna dataskyddsförordning (*UK GDPR*) och dataskyddslagen från år 2018 (*Data Protection Act)*. Denna vägledning är relevant för frågan om utlämnande av kamerabevakningsmaterial till polisen.

Polisen kan begära ut material från kamerabevakning inom ramen för en utredning. Den ovan nämnda vägledningen från Information Commissioner's Office slår fast att det i de flesta fall är lämpligt att lämna ut information från kamerabevakning till brottsbekämpande myndigheter, när kamerabevakningen skett i syfte att bidra till att förebygga och upptäcka brott. Om inte ett domstolsbeslut föreligger finns det emellertid ingen laglig skyldighet för andra aktörer att lämna ut material, utan detta sker i så fall på frivillig grund.

Även om kamerabevakningen i det enskilda fallet inte skett i syfte att förebygga och upptäcka brott är det enligt vägledningen ändå godtagbart att lämna ut information till brottsbekämpande myndigheter om det är relevant för polisens arbetsuppgifter, och om det skulle riskera att skada en pågående brottsutredning att underlåta att lämna ut materialet.

4.4.7 Italien

De italienska polismyndigheterna kan få tillgång till material från bevakningskameror som ägs av andra offentliga organ och privatpersoner på flera grunder.

I allmänhet kan brottsbekämpande myndigheter begära tillgång till material från bevakningskameror så snart det behövs för att utreda brott, men även i syfte att värna allmän säkerhet. En begäran från en polismyndighet om utfående av kamerabevakningsmaterial måste vara motiverad, och polismyndigheten måste antingen få ägarens tillstånd till utlämning (frivilligt utlämnande) eller ha en husrannsakningsorder.

Direktåtkomst för en polismyndighet till material från annans kamerabevakning är möjlig, men i dessa fall är den lagliga grunden för åtkomst antingen uttryckliga lagbestämmelser i särskilda fall, eller en administrativ och bindande överenskommelse mellan två offentliga organ (exempelvis mellan en polismyndighet och en kommun).

4.4.8 Belgien

Den belgiska polisen har ingått avtal med vissa statliga organ för att kunna ta del av material från dessa organs kamerabevakning.

Utöver möjligheten att på denna avtalsmässiga grund få del av material från andra statliga myndigheters och organs kamerabevakning har den belgiska polisen straffprocessuella möjligheter att, inom ramen för en brottsutredning, begära ut eller ta i beslag sådant kamerabevakningsmaterial som är nödvändigt för utredningens bedrivande.

5 Den dataskyddsrättsliga regleringen

5.1 Inledning

Bestämmelser om dataskydd växte fram i Europa under 1970-talet. Denna utveckling skedde först inom ramen för de nationella rättsordningarna, men från och med 1980-talet även på europeisk nivå, bl.a. i och med Europarådets dataskyddskonvention. Bakgrunden till denna rättsutveckling var i hög grad en framväxande uppfattning om att rätten till privatliv utgör en mänsklig rättighet. Dataskyddsreglerna tillkom med det huvudsakliga syftet att värna den personliga integriteten och har sin grund i de mänskliga rättigheterna, framför allt artikel 8 i Europakonventionen och artiklarna 3, 7 och 8 i EU:s rättighetsstadga. Rätten till skydd för personuppgifter är ofta en nödvändig förutsättning för att dessa rättigheter ska kunna garanteras och upprätthållas. Det är mot denna bakgrund och i detta ljus som dataskyddslagstiftningen ska ses. I avsnittet nedan redogörs för EU-rättslig och relevant svensk dataskyddsreglering.

5.2 Den EU-rättsliga dataskyddsregleringen

5.2.1 EU:s dataskyddsreform och dataskyddsförordningen

Det första EU-rättsliga regelverket om dataskydd var 1995 års dataskyddsdirektiv, som var inspirerat av Europarådets dataskyddskonvention. År 2018 genomfördes en genomgripande dataskyddsreform inom EU. 1995 års dataskyddsdirektiv ersattes då av två

rättsakter. Dels dataskyddsförordningen[9], dels dataskyddsdirektivet[10].

Dataskyddsförordningen är direkt tillämplig i alla medlemsstater. Förordningen innehåller en reglering av sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register (artikel 2.1). I artikel 2.2. föreskrivs när förordningen inte ska tillämpas, vilket är bl.a. när behandling av personuppgifter sker av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten (artikel 2.1 d). Av artikel 1.2 framgår att syftet med förordningen bl.a. är att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Det går alltså att utläsa en tydlig koppling till artikel 8 i Europakonventionen och artiklarna 3, 7 och 8 i EU:s rättighetsstadga, liksom till skyddet för personlig integritet i övrigt.

Med *personuppgifter* avses i förordningen varje upplysning som avser en identifierad eller identifierbar fysisk person. En identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet (artikel 4.1).

Vidare framgår av artikel 4.7 att *personuppgiftsansvarig* är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i

[9] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[10] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

unionsrätten eller i medlemsstaternas nationella rätt. En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning är *personuppgiftsbiträde* (artikel 4.8).

Av artikel 5 framgår att vid behandling av personuppgifter ska uppgifterna behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Uppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Säkerställandet ska ske med användning av lämpliga tekniska eller organisatoriska åtgärder.

Artikel 6 stadgar att behandling av personuppgifter endast är laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt.

- Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
- Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
- Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.
- Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

– Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter.

Särskilt om hanteringen av känsliga personuppgifter

Enligt artikel 9 gäller som huvudregel att behandling av känsliga personuppgifter, det vill säga uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning, är förbjuden. Artikeln innehåller dock ett antal undantag från huvudregeln. Undantagen innebär att behandling av känsliga uppgifter kan vara tillåten bl.a. om behandlingen under vissa förutsättningar är *nödvändig* (artikel 9.2).

Av artikel 4.14 framgår att med *biometriska uppgifter* avses personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av den fysiska personen, såsom ansiktsbilder eller fingeravtrycksuppgifter.

Enligt regeringens bedömning i förarbetena utgör endast ett vanligt fotografi, en film eller en annan bild av ett ansikte inte en biometrisk uppgift. Det krävs att bilden eller filmen har bearbetats tekniskt för att möjliggöra igenkänning, t.ex. med hjälp av ett program för automatisk ansiktsigenkänning (jfr prop. 2017/18:232 s. 85 f.). Av skäl 51 till förordningen framgår att behandling av foton inte systematiskt bör anses utgöra behandling av särskilda kategorier av personuppgifter, eftersom foton endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person.

5.2.2 Dataskyddsdirektivet

Allmänt om direktivet

När det gäller behandling av personuppgifter inom brottsbekämpningen ska dataskyddsdirektivet tillämpas i stället för dataskyddsförordningen. Dataskyddsdirektivet är ett s.k. minimidirektiv, vilket innebär att medlemsstaterna är oförhindrade att föreskriva strängare regler för behandling av personuppgifter. Eftersom direktiv inte är direkt tillämpliga i medlemsstaterna behövs en nationell lag som genomför bestämmelserna. Detta har i Sverige skett i huvudsak genom införandet av brottsdatalagen (2018:1177) (se avsnitt 5.3.2).

Liksom dataskyddsförordningen syftar dataskyddsdirektivet bl.a. till att skydda fysiska personers grundläggande fri- och rättigheter, särskilt rätten till skydd av personuppgifter (artikel 1.2 a).

Enligt artikel 1.1 och artikel 2 är direktivet tillämpligt på behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Av artikel 2 framgår vidare att direktivet ska tillämpas dels på helt eller delvis automatiserad behandling av personuppgifter, dels på annan behandling av personuppgifter som ingår i eller kommer att ingå i register. Däremot ska direktivet inte tillämpas på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten eller på personuppgiftsbehandling som utförs av unionens institutioner eller andra organ.

Direktivets begrepp *personuppgifter* har samma betydelse som i dataskyddsförordningen (artikel 3.1).

Begreppet *personuppgiftsansvarig* avser i direktivet en behörig myndighet som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller medlemsstaternas nationella rätt (artikel 3.8). *Personuppgiftsbiträde* beskrivs på samma sätt som i dataskyddsförordningen (artikel 3.9).

Artikel 4 innehåller vissa grundläggande principer för behandling av personuppgifter. Enligt denna artikel ska medlemsstaterna föreskriva att personuppgifterna ska

- behandlas på ett lagligt och korrekt sätt,
- samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte behandlas på ett sätt som står i strid med dessa ändamål,
- vara adekvata, relevanta och inte för omfattande i förhållande till de syften för vilka de behandlas,
- vara korrekta och, om nödvändigt, uppdaterade,
- inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka de behandlas,
- behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna.

Av artikel 4 följer vidare att behandling för något annat ändamål som anges i artikel 1.1 än det för vilket uppgifterna samlats in är tillåten, om den personuppgiftsansvarige har rätt att behandla personuppgifter för ett sådant ändamål och behandlingen är nödvändig och står i proportion till det nya ändamålet. Behandlingen kan inkludera arkivändamål som är av allmänt intresse och vetenskaplig, statistisk eller historisk användning för de ändamål som anges i artikel 1.1, om det finns lämpliga skyddsåtgärder.

Av artikel 5 följer att medlemsstaterna ska föreskriva lämpliga tidsgränser för när personuppgifter ska raderas eller för regelbunden översyn av behovet av att lagra sådana uppgifter, samt att det ska finnas procedurregler som säkerställer att dessa tidsgränser hålls.

Enligt artikel 6 ska den personuppgiftsansvarige så långt möjligt göra åtskillnad mellan personuppgifter som rör olika kategorier av registrerade, såsom misstänkta, dömda, brottsoffer och andra som berörs av brott.

Av artikel 7 framgår att åtskillnad så långt möjligt ska göras mellan personuppgifter som grundar sig på fakta och uppgifter som grundar sig på personliga bedömningar. Behöriga myndigheter ska vidta alla rimliga åtgärder för att se till att personuppgifter som är

felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. Om felaktiga personuppgifter har överförts eller personuppgifter överförts olagligen ska mottagaren omedelbart underrättas om det. I sådana fall ska personuppgifterna rättas eller raderas eller behandlingen av dem begränsas.

Enligt artikel 8 ska medlemsstaterna föreskriva att behandling av personuppgifter är laglig endast om och i den utsträckning behandlingen är nödvändig för att behöriga myndigheter ska kunna utföra sådana uppgifter som anges i artikel 1.1 och som grundas på unionsrätt eller nationell rätt. Den nationella rätten ska åtminstone specificera syftet med behandlingen, vilka personuppgifter som ska behandlas och behandlingens ändamål.

Artikel 9 stadgar bl.a. att personuppgifter som samlas in av behöriga myndigheter för de ändamål som anges i artikel 1.1. i direktivet inte får behandlas för andra ändamål än de för vilka uppgifterna samlats in, såvida inte sådan behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt. Det följer också att när personuppgifter behandlas för andra ändamål än de som anges i artikel 1.1. i direktivet ska dataskyddsförordningen tillämpas i stället för dataskyddsdirektivet, såvida inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten. Om de behöriga myndigheterna har anförtrotts andra uppgifter än dem som anges i artikel 1.1, ska dataskyddsförordningen tillämpas på behandling för sådana ändamål. Det gäller även behandling för arkivändamål som är av allmänt intresse, statistiska ändamål och historiska eller vetenskapliga forskningsändamål.

I artikel 11 föreskrivs att medlemsstaterna ska förbjuda att beslut grundas enbart på automatiserad behandling, inbegripet profilering, om beslutet har negativa rättsliga följder för den registrerade eller i betydande grad påverkar honom eller henne. Ett undantag finns dock om automatisk behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, och det finns lämpliga skyddsåtgärder för den registrerades fri- och rättigheter, åtminstone rätten till mänskligt ingripande från den personuppgiftsansvariges sida. Undantagslöst förbud ska dock, enligt artikel 11.3, gälla för profilering som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter enligt artikel 10 (bl.a. automatisk rasprofilering).

I artikel 13 finns bestämmelser om vilken information som medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska vara skyldig att göra tillgänglig för den registrerade. Det rör sig om uppgifter om a) personuppgiftsansvariges identitet och kontaktuppgifter, b) kontaktuppgifter till dataskyddsombudet, c) ändamålen med personuppgiftsbehandlingen, d) rätten att lämna in klagomål till en tillsynsmyndighet samt tillsynsmyndighetens kontaktuppgifter, och e) rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter och begränsning av behandlingen av personuppgifter som rör den registrerade.

Av artikel 13.3 framgår att medlemsstaterna – i den utsträckning och så länge som en sådan åtgärd är nödvändig och proportionerlig i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen – får begränsa registrerades rätt till information i vissa syften. Sådana syften kan bl.a. vara att undvika att hindra rättsliga utredningar eller förfaranden, undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder, samt skydda andra personers rättigheter och friheter.

Särskilt om hanteringen av känsliga personuppgifter

I artikel 10 i dataskyddsdirektivet regleras behandlingen av känsliga personuppgifter. Precis som i dataskyddsförordningen handlar det i direktivet om uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, samt behandling av genetiska uppgifter, biometriska uppgifter för att unikt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Vad som är *biometriska uppgifter* definieras i artikel 3 i direktivet och utgör i allt väsentligt samma definition som i dataskyddsförordningen.

Till skillnad från dataskyddsförordningen är behandling av känsliga personuppgifter tillåten enligt direktivet endast om behandlingen är *absolut nödvändig* (artikel 10). Av artikeln följer att

det även måste finnas lämpliga skyddsåtgärder för den registrerades rättigheter och friheter, samt att a) behandlingen är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, b) behandlingen sker för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan fysisk person, eller c) behandlingen rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

Kravet på att behandlingen ska vara absolut nödvändig gällde redan före dataskyddsdirektivet. Med hänvisning till skyddet av den grundläggande rätten till respekt för privatlivet, slog EU-domstolen fast att behandling av känsliga personuppgifter enligt 1995 års dataskyddsdirektiv måste vara strikt nödvändig för att vara tillåten (se bl.a. EU-domstolens *dom av den 7 november 2013, IPI v. Geoffrey Englebert m.fl.*, *C-473/12, EU:C:2013:715* och *dom av den 8 april 2014, Digital Rights Ireland Ltd v Ireland, C-293/12, EU:C:2014:238)*.

För att bedöma om en behandling av känsliga personuppgifter är absolut nödvändig krävs att en noggrann avvägning görs mellan allmänhetens intresse och rätten till integritet. Vid en sådan avvägning måste ingå en bedömning av bl.a. risken för missbruk och diskriminering, samt vilka skyddsåtgärder som vidtas (jfr Artikel 29-arbetsgruppen för skydd av personuppgifter, Yttrande om vissa centrala frågor gällande direktivet om brottsbekämpning [EU 2016/680], s. 8). Vid bedömningen ska relevanta mänskliga rättigheter beaktas, t.ex. rätten till privatliv enligt artikel 8 Europakonventionen samt artiklarna 3, 7 och 8 EU:s rättighetsstadga. EU-domstolen har uttalat att lagstiftaren i en medlemsstat är skyldig att undersöka om det finns andra möjliga, mindre långtgående åtgärder som inte inskränker rättigheterna i rättighetsstadgan (EU-domstolens *dom av den 17 oktober 2013, Schwarz mot Stadt Bochum, C-291/12, EU:C:2013:670*).

Det är naturligt att ju känsligare de personuppgifter som behandlas är, desto större hänsyn måste tas till nödvändighetsprincipen. Frågan om förenligheten mellan artikel 10 i direktivet och användning av AI för ansiktsigenkänning har ännu inte prövats av EU-domstolen.

5.2.3 EU:s förordning om artificiell intelligens (AI)

Den 13 mars 2024 antogs texten till den kommande EU-förordningen om AI[11]. Av artikel 1.1 framgår att syftet med förordningen är att förbättra den inre marknadens funktion och främja användningen av människocentrerad och tillförlitlig AI, samtidigt som en hög skyddsnivå säkerställs för hälsa, säkerhet och grundläggande rättigheter som fastställs i stadgan om de grundläggande rättigheterna, inbegripet demokrati, rättsstatsprincipen och miljöskydd, mot de skadliga effekterna av AI-system i unionen, och att stödja innovation.

Förordningen bygger på en riskbaserad metod, där olika AI-system regleras på olika sätt beroende på vilken risk systemet anses utgöra. Med risk avses kombinationen av sannolikheten för skada och denna skadas allvarlighetsgrad (artikel 3.2). Ett exempel på högrisksystem är alla system för biometrisk fjärridentifiering (se skäl 54). Sådana system omfattas därför av strikta krav i förordningen. Definitionen av system för biometrisk fjärr-identifiering är ett AI-system vars syfte är att identifiera fysiska personer utan deras aktiva medverkan, vanligtvis på distans, genom jämförelse av en persons biometriska uppgifter med biometriska uppgifter i en referensdatabas (artikel 3.41). Användning av biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpande ändamål är som utgångspunkt inte tillåten. Med realtid avses att insamling av biometriska uppgifter, jämförelse och identifiering sker utan betydande dröjsmål och omfattar inte bara omedelbar identifiering utan även begränsade korta fördröjningar för att undvika kringgående (artikel 3.42).

Av artikel 5 framgår att medlemsstaterna får föreskriva att biometrisk fjärridentifiering i realtid för brottsbekämpande ändamål får användas, under vissa förutsättningar, endast när det är absolut nödvändigt i vissa begränsade situationer, bl.a. när det är nödvändigt för att söka efter ett försvunnet barn, för att förhindra ett specifikt och överhängande terroristhot eller för att upptäcka, lokalisera, identifiera eller lagföra en förövare eller misstänkt för ett allvarligt

[11] Europaparlamentets ståndpunkt fastställd vid första behandlingen den 13 mars 2024 inför antagandet av Europaparlamentets och rådets förordning (EU) 2024/… om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (rättsakt om artificiell intelligens).

brott. För att få använda ett sådant system krävs som utgångspunkt tillstånd från ett rättsligt eller annat oberoende organ. Det krävs även lämpliga begränsningar i tid, geografisk räckvidd och de databaser som har sökts. Artikeln reglerar också hur utdata från systemet för biometrisk fjärridentifiering i realtid får användas.

Förordningen påverkar inte tillämpningen av befintlig unionslagstiftning om behandling av personuppgifter (se skäl 10). Det ankommer på medlemsstaterna att inrätta och/eller utse myndigheter som i olika avseenden har i uppdrag att säkerställa att förordningen efterlevs (artikel 70). Kommissionen beslutade den 24 januari 2024[12] att inrätta en europeisk AI-byrå som ska övervaka efterlevnaden och genomförandet av förordningen. AI-byrån har även som uppdrag att utveckla unionens expertis och kapacitet på AI-området (se skäl 148).

5.3 Den svenska dataskyddslagstiftningen

5.3.1 Allmänt om den svenska regleringen

Den första svenska dataskyddsregleringen var 1973 års datalag, som tillkom på förslag av 1966 års *Integritetsskyddskommitté*. Samtidigt som lagen tillkom inrättades också den nya myndigheten Datainspektionen, numera Integritetsskyddsmyndigheten. I en internationell jämförelse var Sverige förhållandevis tidigt med att utforma dataskyddsregler i syfte att värna enskildas rätt till personlig integritet.

Grundtanken i datalagen var att register över personuppgifter endast fick föras efter tillstånd från Datainspektionen (2 § datalagen) och för bestämda ändamål (5 § datalagen), samt att Datainspektionen skulle utöva tillsyn över automatisk databehandling för att säkerställa att den inte innebar otillbörligt intrång i den personliga integriteten (13 § datalagen).

Gällande datalagens uppbyggnad var registerbegreppet centralt. Med personregister avsågs register, förteckning eller andra anteckningar som förs med hjälp av automatisk databehandling och som kan hänföras till den som avses med uppgiften (1 § datalagen). Med tiden kom datalagens registerbegrepp att kritiseras, eftersom

[12] Kommissionens beslut av den 24 januari 2024 om inrättande av Europeiska byrån för artificiell intelligens C(2024) 390.

det inte fångade in eller i vart fall inte synes fånga in alla typer av behandling av personuppgifter (prop. 2017/18:232 s. 42). Dessutom hade Sverige efter EU-inträdet blivit skyldig att implementera 1995 års dataskyddsdirektiv. Direktivet genomfördes i Sverige genom personuppgiftslagen (1998:204), som därmed ersatte datalagen. I personuppgiftslagen ersattes datalagens registerbegrepp med uttrycket behandling av personuppgifter, i linje med terminologin i 1995 års dataskyddsdirektiv.

Personuppgiftslagen upphävdes i sin tur i samband med EU:s dataskyddsreform år 2018. Eftersom dataskyddsförordningen är direkt tillämplig i medlemsstaterna behövdes personuppgiftslagen inte ersättas. Emellertid infördes en lag med vissa kompletterande bestämmelser till dataskyddsförordningen (lagen [2018:218] med kompletterande bestämmelser till EU:s dataskyddsförordning [dataskyddslagen]). För att genomföra dataskyddsdirektivet i svensk rätt infördes brottsdatalagen (2018:1177). Därutöver finns bestämmelser om personuppgiftshantering bl.a. i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område (polisens brottsdatalag) och lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter (säkerhetspolisens datalag).

5.3.2 Brottsdatalagen

Översikt över lagen

Brottsdatalagen innehåller bestämmelser om bl.a. grundläggande krav på personuppgiftsbehandling, den personuppgiftsansvariges skyldigheter, enskildas rättigheter, skadestånd, överklagande och överföring av personuppgifter till länder utanför EU på områdena brottsbekämpning och upprätthållande av allmän ordning och säkerhet.

I 1 kap. finns bl.a. bestämmelser om lagens syfte och tillämpningsområde. Av 1 kap. 2 § framgår att lagen, i likhet med dataskyddsdirektivet, är tillämplig på behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Lagen gäller också vid behandling

av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet.

Personuppgiftsbehandling som sker i andra syften omfattas inte av brottsdatalagen. Då är i stället dataskyddsförordningen och lagen med kompletterande bestämmelser till EU:s dataskyddsförordning tillämpliga (samt i förekommande fall andra lagar). Utöver brottsdatalagen finns särskilda registerförfattningar med specialbestämmelser för myndigheter som behandlar personuppgifter på brottsdatalagens område. Författningarna tar hänsyn till de särskilda behov som dessa myndigheter har av att kunna behandla personuppgifter för att utföra sina arbetsuppgifter. Registerförfattningarna gäller utöver brottsdatalagen och innehåller preciseringar, undantag eller avvikelser från lagen. För Polismyndigheten samt i viss mån Ekobrottsmyndigheten och Säkerhetspolisen gäller polisens brottsdatalag, med tillhörande förordning (2018:1942).

I 2 kap. brottsdatalagen finns bestämmelser om grundläggande krav på personuppgiftsbehandling. Dessa bestämmelser motsvarar de krav på medlemsstaterna som återfinns i dataskyddsdirektivet. De centrala bestämmelserna i 2 kap. är 1 § som anger de tillåtna rättsliga grunderna för personuppgiftsbehandling och 3 § som ställer upp ett krav på ett uttryckligt angivet berättigat ändamål för personuppgiftsbehandlingen.

I 2 kap. 1 § första stycket stadgas att personuppgifter får behandlas, om det är nödvändigt för att en behörig myndighet ska kunna utföra sin uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. EU-domstolen har i ett avgörande kommit fram till att ordet ”nödvändig” ska tolkas som att det är fråga om något som behövs för att på ett effektivt sätt kunna utföra arbetsuppgiften (*dom av den 16 december 2008, Heinz Huber v Bundesrepublik Deutschland, C-524/06, EU:C:2008:724*). Av paragrafens andra stycke framgår att med en behörig myndighets uppgift avses en uppgift som framgår av lag, förordning eller särskilt regeringsbeslut.

Enligt 2 kap. 3 § får personuppgifter bara behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Om det ändamål som personuppgifterna behandlas för inte framgår av sammanhanget eller på annat sätt, ska det tydliggöras genom en särskild upplysning.

Ändamålet med behandlingen av personuppgifter ska således vara definierat innan behandlingen påbörjas.

Rättslig grund för behandling av personuppgifter och berättigat ändamål för behandling av personuppgifter är olika saker. För att ändamålet med behandlingen ska vara berättigat krävs dock en koppling till en rättslig grund. Kravet på att ändamålet för behandlingen ska vara berättigat kan också sägas innebära ett krav på att behandlingen ska vara förenlig med konstitutionella och andra rättsliga principer. Det finns inget som hindrar att flera parallella berättigade ändamål samtidigt är för handen. (Se prop. 2017/18:232 s. 115.)

Av 2 kap. 4 § första stycket framgår att innan personuppgifter får behandlas för ett nytt ändamål, det vill säga ett annat ändamål än det ändamål för vilket uppgifterna ursprungligen samlats in och behandlats, ska det säkerställas att det finns en rättslig grund enligt 1 § för den nya behandlingen, och att det är nödvändigt och proportionerligt att personuppgifterna behandlas även för det nya ändamålet. Av paragrafens andra stycke framgår att i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning ska någon prövning enligt första stycket inte göras.

Bestämmelsen i 2 kap. 4 § första stycket motsvarar i huvudsak artikel 4 i dataskyddsdirektivet och innebär att varje behandling av personuppgifter för ett visst nytt ändamål ska nå upp till samma rättsliga krav, oavsett om behandlingen avser personuppgifter som samlats in särskilt för det ändamålet, eller uppgifter som samlats in för något annat sammanhang och något annat ändamål. Här avses behandling av personuppgifter inom brottsdatalagens tillämpningsområde (jfr prop. 2017/18:232 s. 442). När det handlar om att behandla personuppgifter som ursprungligen samlats in och behandlats enligt brottsdatalagen för ändamål utanför lagens tillämpningsområde gäller i stället 2 kap. 22 §. I sistnämnda paragraf föreskrivs att det ska säkerställas att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det ändamål som ligger utanför lagens tillämpningsområde (exempelvis inom dataskyddsförordningens område). I den utsträckning det i lag eller förordning är föreskrivet en skyldighet att lämna ut personuppgifter ska någon sådan prövning inte göras.

I 2 kap. 6 § stadgas att personuppgifter ska behandlas författningsenligt och på ett korrekt sätt. Av 7 § framgår att person-

uppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade. Det framgår även att uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet. Syftet med den senare bestämmelsen är att förhindra att personers utseende beskrivs i ordalag som kan vara kränkande för individen (prop. 2017/18:232 s. 444).

Av 2 kap. 8 § framgår att personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

I 2 kap. 9 § föreskrivs att olika kategorier av personuppgifter så långt det är möjligt ska särskiljas så att det framgår om personen är misstänkt, dömd för brott, brottsoffer eller någon annan som berörs av ett brott. I 2 kap. 10 § stadgas att personuppgifter som grundar sig på fakta så långt det är möjligt ska särskiljas från personuppgifter som grundar sig på personliga bedömningar. Bestämmelsen motsvarar i huvudsak artikel 7 i dataskyddsdirektivet. I 17 § första stycket föreskrivs att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen, den s.k. lagringsminimeringsprincipen.

Särskilt om hanteringen känsliga personuppgifter

Bestämmelser om behandling av känsliga personuppgifter finns i 2 kap. 11–14 §§. Dessa bestämmelser genomför, och motsvarar i huvudsak, artikel 10 i dataskyddsdirektivet.

I 2 kap. 11 § första stycket föreskrivs att personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning inte får behandlas. Av andra stycket framgår att personuppgifter som behandlas dock får kompletteras med sådana känsliga personuppgifter, när det är absolut nödvändigt för ändamålet med behandlingen. Andra stycket utgör således ett undantag från första styckets förbud mot behandling av vissa känsliga personuppgifter. Undantaget innebär bl.a. att om andra uppgifter om en person samlas in i samband med t.ex. en förundersökning får de kompletteras med uppgifter om religiös övertygelse eller etniskt ursprung, om det är av betydelse för

utredningen, exempelvis för att utreda hets mot folkgrupp. Vidare kan det under utredning av sexualbrott ibland vara befogat att anteckna uppgifter om den misstänktes sexualliv. (Se prop. 2017/18:232 s. 447.)

Av 2 kap. 12 § framgår att biometriska och genetiska uppgifter endast får behandlas, om det är särskilt föreskrivet och absolut nödvändigt för ändamålet med behandlingen. För Polismyndighetens, och i vissa situationer Säkerhetspolisens, vidkommande finns en sådan särskild föreskrift i 2 kap. 4 § polisens brottsdatalag (se avsnitt 5.3.3).

Biometriska uppgifter definieras i 1 kap. 6 § på motsvarande sätt som i artikel 3 i dataskyddsdirektivet som personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen.

Av 2 kap. 14 § framgår att det är förbjudet att göra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Det är alltså som utgångspunkt inte tillåtet att söka fram listor med t.ex. personer med en särskild etnicitet. I polisens brottsdatalag finns dock vissa undantag från detta sökförbud (se avsnitt 5.3.3).

I 3 kap. finns bestämmelser om den personuppgiftsansvariges skyldigheter. Personuppgiftsansvarig definieras i 1 kap. 6 § som den behöriga myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Av 3 kap. 1 § följer att den personuppgiftsansvarige är ansvarig för all behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar. I 2–5 och 8 §§ finns bestämmelser om att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att personuppgiftsbehandlingen är författningsenlig och att den registrerades rättigheter skyddas. Enligt 6 § ska den personuppgiftsansvarige se till att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

5.3.3 Polisens brottsdatalag

Översikt över lagen

Polisens brottsdatalag är en av de registerförfattningar som kompletterar brottsdatalagen i särskilda fall, bl.a. vad avser vissa myndigheters behandling av personuppgifter.

Lagens tillämpningsområde anges i 1 kap. 1 och 2 §§. Av 1 § framgår att lagen ska tillämpas av Polismyndigheten, när den behandlar personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd eller upprätthålla allmän ordning och säkerhet. Lagen gäller också för Säkerhetspolisen i frågor som inte rör nationell säkerhet, om uppgifterna behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. Lagen gäller även för Ekobrottsmyndigheten i vissa situationer. För Ekobrottsmyndigheten och Säkerhetspolisen gäller endast 1–4 och 7 kap.

I 1 kap. 2 § framgår att lagen inte gäller vid Polismyndighetens behandling av personuppgifter enligt vapenlagen (1996:67), lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2006:444) om passagerarregister, eller lagen (2014:400) om Polismyndighetens elimineringsdatabas. I dessa lagar finns särskilda regler om Polismyndighetens behandling av personuppgifter, som är tillämpliga i stället för polisens brottsdatalag. Enligt samma bestämmelse gäller lagen inte heller vid behandling av personuppgifter enligt Europaparlamentets och rådets förordningar (EU) 2018/1861 och (EU) 2018/1862 om inrättande, drift och användning av Schengens informationssystem (SIS) på vissa områden och inte heller vid behandling enligt lagen (2021:1187) med kompletterande bestämmelser till EU:s förordningar om Schengens informationssystem och föreskrifter som har meddelats i anslutning till den lagen. Enligt beslutade men ännu inte ikraftträdda ändringar i 1 kap. 2 § polisens brottsdatalag gäller lagen vid behandling av personuppgifter enligt Europaparlamentets och rådets förordning (EU) 2017/2226 om inrättande av ett gemensamt in- och utresesystem för registrering av uppgifter om tredjelandsmedborgare. Ändringarna träder i kraft den dag som regeringen bestämmer.

Säkerhetspolisens behandling av personuppgifter i verksamhet som rör nationell säkerhet faller helt utanför EU-rättens område och

omfattas varken av dataskyddslagen eller brottsdatalagen. För behandling av personuppgifter i sådan verksamhet tillämpas i stället säkerhetspolisens datalag (se avsnitt 5.3.4).

I 2 kap. polisens brottsdatalag finns de grundläggande reglerna om polisens behandling av personuppgifter. I 1 § föreskrivs den rättsliga grunden för polisens behandling av personuppgifter enligt lagens tillämpningsområde. Där framgår att personuppgifter får behandlas, om det är nödvändigt för att en behörig myndighet ska kunna utföra en uppgift bestående i att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd, upprätthålla allmän ordning och säkerhet, eller fullgöra förpliktelser som följer av internationella åtaganden. Av 2 § framgår att förutsättningarna för att behandla personuppgifter för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (se avsnitt 5.3.2).

I 2 kap. 7–14 §§ finns bestämmelser om utlämnande av personuppgifter i vissa fall, såväl utlämnande från Polismyndigheten och Säkerhetspolisen som utlämnande till dessa myndigheter. Genom bestämmelserna bryts viss sekretess som annars skulle ha gällt enligt offentlighets- och sekretesslagen (2009:400) (OSL). I 2 kap. 8 § regleras t.ex. de brottsbekämpande myndigheternas rätt att, trots sekretess till skydd för enskild enligt 21 kap. 3 § första stycket OSL (viss sekretess till skydd för förföljda personer) och 35 kap. 1 § OSL (sekretess till skydd för enskild i bl.a. förundersökning), i den brottsbekämpande verksamheten få del av personuppgifter som har gjorts gemensamt tillgängliga enligt 3 kap. 2 § polisens brottsdatalag.

I 3 kap. polisens brottsdatalag finns bestämmelser om behandling av personuppgifter som har gjorts gemensamt tillgängliga. Med att uppgifter gjorts gemensamt tillgängliga avses att de gjorts tillgängliga för en vidare personkrets inom en myndighet, t.ex. (men inte endast) i form av en sökbar databas. Om avsikten är att uppgifterna ska vara åtkomliga för en i förväg obestämd krets av anställda, får uppgifterna alltid anses vara gemensamt tillgängliga. Exempel på detta är uppgifter i polisens nationella uppgiftssamlingar, men även lokala register där det inte på förhand har bestämts vilka personer som får ha tillgång till uppgifterna. Att olika personalkategorier kan ha olika behörighet, och att en uppgift därför i praktiken vid en viss tidpunkt är åtkomlig enbart för ett begränsat antal personer, innebär alltså inte att uppgiften inte kan anses vara

gemensamt tillgänglig. Uppgifter som en annan brottsbekämpande myndighet har tillgång till genom direktåtkomst är alltid gemensamt tillgängliga. Om uppgifterna å andra sidan lagras på ett sådant sätt att endast en viss person har tillgång till dem, kan uppgifterna normalt inte anses gemensamt tillgängliga. (Se prop. 2009/10:85 s. 334.) En tumregel för hur många personer som kan ha tillgång till uppgifterna utan att de anses ha gjorts gemensamt tillgängliga är ett tiotal (a. prop. s. 128 f.).

I 3 kap. 2 § framgår vilka personuppgifter som får göras gemensamt tillgängliga. Som exempel kan nämnas uppgifter som kan antas ha samband med misstänkt brottslig verksamhet, om den misstänkta verksamheten antingen innefattar brott för vilket det är föreskrivet fängelse i ett år eller mer, eller sker systematiskt (p. 1). Därutöver får också bl.a. uppgifter som behövs för övervakningen av en person som kan antas komma att begå brott för vilket det är föreskrivet fängelse i två år eller mer, och som är allvarligt kriminellt belastad eller kan antas utgöra ett hot mot andras personliga säkerhet göras gemensamt tillgänglig (p. 2). Vidare får alla uppgifter som förekommer i ett ärende om utredning av eller lagföring för brott göras gemensamt tillgängliga (p. 3), liksom uppgifter som har rapporterats till Polismyndighetens ledningscentraler och uppgifter som behandlas i syfte att upprätthålla allmän ordning och säkerhet (p. 6 och 7). Därutöver föreskrivs i paragrafen ytterligare situationer när uppgifter får göras gemensamt tillgängliga.

I 3 kap. 3 och 4 §§ finns bestämmelser om att personuppgifter som har gjorts gemensamt tillgängliga ska förses med särskilda upplysningar. I 3 kap. 5 § föreskrivs en allmän begränsning av vilka uppgifter som får tas fram vid sökning i gemensamt tillgängliga uppgifter på namn, personnummer, samordningsnummer eller liknande identitetsbeteckningar. Exempelvis får uppgifter tas fram som visar att den sökta personen är anmäld för brott eller är eller har varit misstänkt för brott (3 kap. 5 § första stycket 1 och 2).

I 3 kap. 7 § finns en bestämmelse som möjliggör direktåtkomst för de brottsbekämpande myndigheterna till varandras gemensamt tillgängliggjorda uppgifter, om direktåtkomsten sker i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder, eller upprätthålla allmän ordning och säkerhet.

I 4 kap. finns bestämmelser med tidsgränser för hur länge personuppgifter får behandlas. Tidsgränserna kompletterar och konkretiserar den allmänna bestämmelsen i 2 kap. 17 § brottsdatalagen som föreskriver att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

Av 4 kap. 2 § polisens brottsdatalag framgår att personuppgifter som inte har gjorts gemensamt tillgängliga inte får behandlas längre än ett år efter det att ärendet avslutades, om de behandlas i ett ärende, eller ett år efter det att de behandlades automatiserat första gången, om de inte kan hänföras till ett ärende. I 7–11 §§ finns bestämmelser om den längsta tid under vilken personuppgifter som har gjorts gemensamt tillgängliga får behandlas. Den längsta tillåtna tiden för att behandla personuppgifterna varierar beroende på vilken grund i 3 kap. 2 § som uppgifterna gjorts gemensamt tillgängliga. När det gäller uppgifter som gjorts gemensamt tillgängliga på den grunden att de kan antas ha samband med misstänkt brottslig verksamhet som antingen innefattar brott för vilket det är föreskrivet fängelse i ett år eller mer eller som sker systematiskt får de enligt 4 kap. 7 § första stycket alltid behandlas i vart fall ett år efter det att ärendet avslutades. Enligt andra stycket får personuppgifter som gjorts gemensamt tillgängliga på samma grund men som inte behandlas i ett ärende inte behandlas längre än tre år efter utgången av det kalenderår då registreringen avseende personen gjordes. Personuppgifter som kan antas ha samband med brottslig verksamhet som innefattar brott för vilket det är föreskrivet fängelse i två år eller mer får inte behandlas längre än fem år efter utgången av det kalenderår då registreringen gjordes.

I 5 kap. finns bestämmelser om de behöriga myndigheternas rätt att föra olika typer av register, däribland polisens register över dnaprofiler, fingeravtryck och signalement. Uppgifter om misstänkta och dömda får inte sammanblandas i dessa register (jfr 2 kap. 9 § brottsdatalagen).

Särskilt om hanteringen av känsliga personuppgifter

Bestämmelser om behandling av känsliga personuppgifter finns i 2 kap. 4–6 §§ polisens brottsdatalag. Av 2 kap. 4 § framgår att Polis-

myndigheten och Säkerhetspolisen får behandla biometriska uppgifter, om det är absolut nödvändigt för ändamålet med behandlingen. Denna bestämmelse är en sådan särskild föreskrift som avses i 2 kap. 12 § brottsdatalagen och ger lagligt stöd för Polismyndigheten och Säkerhetspolisen att använda t.ex. fingeravtryck, ansiktsgeometri, röstigenkänning eller rörelsemönster för att identifiera en person. Behovet av att behandla sådana uppgifter måste prövas särskilt noga. (Se prop. 2017/18:269 s. 296.) Särskild hänsyn måste tas till i vilken mån motsvarande ändamål kan uppnås med en mindre omfattande behandling av personuppgifter.

I 2 kap. 5 och 6 §§ polisens brottsdatalag finns vissa undantag från förbudet i 2 kap. 14 § brottsdatalagen mot att söka på känsliga personuppgifter. Av 5 § framgår att sökförbudet inte hindrar att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott, uppgifter om verkställighet av påföljd eller uppgifter som beskriver en persons utseende används som sökbegrepp, även om det skulle leda till ett urval av personer grundat på känsliga personuppgifter som t.ex. hälsa eller sexuell läggning.

I 6 kap. polisens brottsdatalag finns särskilda bestämmelser om hantering av känsliga personuppgifter i den forensiska verksamheten. Inom ramen för forensisk verksamhet gäller dessa bestämmelser i stället för 2–4 kap. polisens brottsdatalag. Forensisk verksamhet är ett sammanfattande begrepp för utveckling och tillämpning av metoder från olika vetenskapliga ämnesområden – t.ex. biologi, kemi eller teknologi – på frågeställningar om framför allt olika typer av fysiska spår som undersöks med anledning av misstanke om brott. All identifiering av t.ex. misstänka gärningspersoner utgör dock inte forensisk verksamhet. Forensisk verksamhet ställer särskilda krav på oberoende och vetenskaplig grund. Det är alltså bara de åtgärder som vilar på sådan grund som kan sägas vara forensiska åtgärder. I kravet på oberoende ligger bl.a. att forensiska undersökningar, analyser och jämförelser ska hanteras helt separat från annat utredningsarbete under en förundersökning (se t.ex. prop. 2017/18:269 s. 169). Detta innebär att åtgärder som vidtas av brottsbekämpande myndigheter inom ramen för ordinärt utredningsarbete typiskt sett inte är att anse som forensisk verksamhet. Gränsdragningen mellan forensiska ändamål och brottsbekämpande ändamål diskuteras utförligt i prop. 2014/14:94 s. 56 f.

5.3.4 Säkerhetspolisens datalag

Som framgått ovan är brottsdatalagen och polisens brottsdatalag tillämpliga när Säkerhetspolisen behandlar personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. Däremot är brottsdatalagen och polisens brottsdatalag inte tillämpliga på personuppgiftsbehandling som rör nationell säkerhet. Området nationell säkerhet omfattas överhuvudtaget inte av unionsrätten, varför inte heller dataskyddsförordningen eller dataskyddsdirektivet är tillämpliga på personuppgiftsbehandling på det området.

När Säkerhetspolisen i sin brottsbekämpande och lagförande verksamhet behandlar personuppgifter som rör nationell säkerhet är i stället säkerhetspolisens datalag tillämplig. Lagen innehåller bestämmelser om bl.a. grundläggande krav på personuppgiftsbehandling, den personuppgiftsansvariges skyldigheter, enskildas rättigheter, skadestånd, överklagande och överföring av personuppgifter till tredjeland. Dessa bestämmelser överensstämmer i stort med brottsdatalagens bestämmelser.

6 Kamerabevakning

6.1 Inledning

Kamerabevakning kan bedrivas på olika sätt och av olika aktörer. Möjligheterna för en aktör att bedriva kamerabevakning på en plats dit allmänheten har tillträde regleras i de flesta fall i kamerabevakningslagen (2018:1200). I avsnittet redogörs för kamerabevakningslagen, regleringen av personuppgiftsbehandling av uppgifter som samlas in genom kamerabevakning, kamerabevakning med ANPR-teknik och vissa myndigheters användning av kamerabevakning.

6.2 Kamerabevakningslagen

När kamerabevakningslagen infördes framhöll regeringen att kamerabevakning kan vara särskilt betydelsefull i de brottsbekämpande myndigheternas verksamhet. På allmänna platser kan tekniken fungera som ett viktigt komplement till andra brottsförebyggande åtgärder. Regeringen anförde att kamerabevakning kan underlätta avslöjandet av pågående brott och vara av avgörande betydelse i efterföljande utredningar. (Se prop. 2017/18:231 s. 31.) I det operativa brottsbekämpande arbetet har kamerabevakning en stor betydelse. Kamerabevakning kan ge en lägesbild över ett visst område, och en uppfattning exempelvis om var folksamlingar uppstår och var olika personer vistas. Därigenom ges goda förutsättningar att ingripa och avstyra nära förestående eller pågående brottslighet. När en utveckling kan följas på detta sätt kan bl.a. Polismyndigheten förbereda sina insatser bättre och anpassa dem till den rådande situationen, t.ex. genom att ingripa med rätt personalstyrka. Denna möjlighet har stor betydelse vid brottslighet i utsatta områden. (Se prop. 2018/19:147 s. 25.)

Kamerabevakningslagens syfte är att tillgodose behovet av kamerabevakning för berättigade ändamål och att skydda fysiska personer mot otillbörligt intrång i den personliga integriteten vid sådan bevakning (2 §). Avsikten med lagen är alltså att reglera kamerabevakning på ett sätt som innebär en lämplig balans mellan nyttan med kamerabevakning och skyddet av den personliga integriteten (prop. 2017/18:231 s. 135).

Med kamerabevakning avses i lagen att en tv-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning, utan att manövreras på platsen, används på ett sätt som innebär varaktig eller regelbundet upprepad personbevakning (3 §). Med platsen menas den plats där utrustningen finns. Utrustningen kan finnas antingen på en fast plats, t.ex. på en fasad, på en inomhusvägg, i ett tak eller på en stolpe, eller på en rörlig plats, t.ex. på eller i ett fordon, ett fartyg eller en drönare eller ett annat luftfartyg. Med att utrustningen används utan att manövreras på platsen avses att den fortlöpande hanteringen av utrustningen sker på ett ställe som är klart åtskilt från den plats där utrustningen finns. Endast det förhållandet att utrustningen sätts i gång på stället eller fungerar med inbyggd automatik innebär inte att den manövreras på platsen. Utrustning som finns i användarens omedelbara närhet och som fortlöpande styrs av användaren är däremot manövrerad på platsen. Lagen omfattar därför inte exempelvis handhållna eller kroppsburna kameror. (Se prop. 2017/18:231 s. 136.)

En förutsättning för att lagen ska vara tillämplig är att kamerabevakningen används på ett sådant sätt att det är möjligt att identifiera personer som blir föremål för bevakningen, det vill säga att det är fråga om personbevakning. Det förutsätts också att bevakningen pågår under en viss tid eller med vissa regelbundna intervaller (prop. 2017/18:231 s. 136).

Kamerabevakningslagen gäller även i fråga om ljudupptagning som sker i anslutning till kamerabevakningen, liksom vid användning av tekniska anordningar som används för att behandla bild- och ljudmaterial (3 § 2 och 3).

Som huvudregel krävs tillstånd till kamerabevakning, om bevakningen ska bedrivas av en myndighet eller annan än myndighet vid utförande av en uppgift av allmänt intresse och av en plats dit allmänheten har tillträde (7 §). Till platser dit allmänheten har tillträde räknas exempelvis gator, torg och parker, men också

transportmedel som används för allmänna kommunikationer eller evenemang dit vem som helst kan lösa en biljett (prop. 2017/18:231 s. 59).

Av 5 § framgår att lagen bl.a. inte gäller vid hemlig kameraövervakning enligt 27 kap. RB eller lagen om åtgärder för att förhindra vissa särskilt allvarliga brott.

Sedan den 1 januari 2020 krävs inget tillstånd till kamerabevakning som bedrivs av Kustbevakningen, Polismyndigheten, Säkerhetspolisen eller Tullverket (9 § första stycket 1). Tillståndskravet togs bort för att förbättra dessa myndigheters möjlighet att bekämpa och lagföra brott med hjälp av kamerabevakning (prop. 2018/19:147 s. 1).

Trots undantaget från tillståndskravet är som huvudregel en förutsättning för att de uppräknade myndigheterna ska få bedriva kamerabevakning av en plats dit allmänheten har tillträde att intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad. Vid denna bedömning ska 8 § andra och tredje styckena tillämpas (14 a §) (se vidare avsnitt 6.2.1). Enligt 14 b § ska en dokumenterad bedömning av om förutsättningarna i 14 a § är uppfyllda göras innan myndigheten påbörjar kamerabevakningen. En ny dokumenterad bedömning ska göras innan myndigheten ändrar bevakningen på ett betydande sätt som ökar risken för intrång i den enskildes personliga integritet. Detsamma gäller om förhållandena på den plats som bevakas ändras på ett betydande sätt som minskar intresset av bevakningen eller ökar risken för intrång i den enskildes personliga integritet.

Viss typ av kamerabevakning är undantagen från kravet på en dokumenterad intresseavvägning, exempelvis Polismyndighetens kamerabevakning vid automatisk hastighetsövervakning och i gränsnära områden samt bevakning av vissa i 9 § utpekade platser när bevakningen har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott (14 c §). I 14 d § finns ytterligare undantag från kravet på tillstånd och att en dokumenterad intresseavvägning ska göras gällande viss tidsbegränsad kamerabevakning. Det gäller bl.a. kamerabevakning som Polismyndigheten eller Säkerhetspolisen bedriver under högst tre månader, om det av särskild anledning finns risk för allvarlig brottslighet och syftet med bevakningen är att förebygga, förhindra

eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott.

Enligt 15 § första stycket ska en upplysning om kamerabevakning lämnas genom tydlig skyltning eller på något annat verksamt sätt. I andra stycket föreskrivs att om ljud kan avlyssnas eller tas upp vid bevakningen, ska en särskild upplysning lämnas om detta. I tredje stycket finns en upplysning om att bestämmelser om rätten till information om den personuppgiftsbehandling som kamerabevakningen innebär finns i dataskyddsförordningen och andra föreskrifter som anges i 6 §.

Det är viktigt från integritetssynpunkt att den som blir bevakad informeras om bevakningen på ett tydligt sätt. Detta möjliggör för enskilda att anpassa sig till att platsen är kamerabevakad och, i många fall, välja om de vill bli föremål för sådan övervakning. Att bevakningen är känd är också av avgörande betydelse för att den ska vara effektiv i brottsförebyggande syfte. (Se prop. 2017/18:231 s. 88.)

Det vanligaste sättet att uppfylla kravet på upplysning är genom tydlig skyltning i direkt anslutning till den plats som kamerabevakas. Upplysningsplikten ersätter inte de allmänna regler om information som finns i dataskyddsförordningen och brottsdatalagen. Sådan ytterligare information kan lämnas på en skylt som upplyser om kamerabevakningen men kan också göras tillgänglig på något annat sätt, exempelvis genom en hänvisning till en webbsida (prop. 2018/19:147 s. 18).

Från upplysningsplikten finns vissa undantag reglerade i 16 och 17 §§. Av 16 § första stycket framgår bl.a. att upplysning om kamerabevakning och information om den personuppgiftsbehandling som kamerabevakningen innebär inte behöver lämnas vid bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning eller vid bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för allvarlig brottslighet och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott. Av 16 § andra stycket framgår att undantagen i första stycket inte gäller om ljud ska avlyssnas eller tas upp vid kamerabevakningen. Av 17 § framgår att tillsynsmyndigheten, om det finns synnerliga skäl, får besluta i enskilda fall om undantag från upplysningskravet och rätten

till information om den personuppgiftsbehandling som kamerabevakningen innebär. Undantagen tillkom bl.a. med hänvisning till att integritetsintrånget i vissa fall är begränsat och att själva syftet med bevakningen skulle motverkas genom ett ovillkorligt krav på upplysning (se bl.a. prop. 1989/90:119 s. 30).

Kamerabevakningslagen innehåller även bestämmelser om bl.a. tillsyn, sanktionsavgifter och skadestånd (23–28 §§). Integritetsskyddsmyndigheten är den myndighet som utövar tillsyn över kamerabevakning enligt kamerabevakningslagen (2 § förordningen [2007:975] med instruktion för Integritetsskyddsmyndigheten).

6.2.1 Särskilt om intresseavvägningen

I de fall det vid kamerabevakning ska göras en intresseavvägning enligt 8 § kamerabevakningslagen ska det enligt paragrafens andra stycke särskilt beaktas om bevakningen behövs för att

1) förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats eller på en annan plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet eller på egendom,

2) förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller begränsa verkningarna av sådana störningar,

3) utöva kontrollverksamhet,

4) förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor, eller

5) tillgodose andra därmed jämförliga ändamål.

Vid bedömningen av den enskildes intresse av att inte bli bevakad ska, enligt tredje stycket i samma paragraf, särskilt beaktas

1.) hur bevakningen ska utföras,

2.) om teknik som främjar skyddet av den enskildes personliga integritet ska användas, och

3.) vilket område som ska bevakas.

Gällande punkten 1 i första stycket tar den inte enbart sikte på brott som begås på platsen eller brott som redan har begåtts. Även kamerabevakning som sker inom ramen för underrättelseverksamhet omfattas av bestämmelsen (SOU 2021:92 s. 315). Med en brottsutsatt plats menas en plats där det finns problem med brottslighet. Med detta avses inte varje plats där det någon gång har inträffat enstaka brott. Däremot krävs inte att brottsligheten är ovanligt hög på platsen i förhållande till andra jämförbara platser för att platsen ska betraktas som brottsutsatt. Exempel på platser som förutsätts vara brottsutsatta är bl.a. knutpunkter för allmänna kommunikationer. (Se prop. 2017/18:231 s. 143.)

De ändamål som räknas upp i 8 § andra stycket är inte uttömmande. Även bevakning för andra ändamål kan komma i fråga, så länge de kan anses vara berättigade och intresset av bevakningen väger tyngre än integritetsintresset i det enskilda fallet. Om kamerabevakning ska bedrivas i situationer som inte nämns uttryckligen i bestämmelsen kan det dock krävas mer ingående överväganden av behovet av kamerabevakning i förhållande till integritetsriskerna och av hur dessa risker kan minskas. (Se prop. 2017/18:231 s. 70 och 144.)

För att bevakningsintresset ska kunna väga tyngre än den enskildes intresse av att inte bli bevakad är en första förutsättning att det finns en rättslig grund för kamerabevakningen i den tillämpliga personuppgiftsregleringen. Därutöver ska en helhetsbedömning av omständigheterna i det enskilda fallet göras. Det räcker att intresset av kamerabevakning väger över det motstående intresset för att tillstånd ska ges. (Se a. prop. s. 142.)

I förarbetena till kamerabevakningslagen uttalade regeringen att det var angeläget att lagstiftningen på ett tydligare sätt tar hänsyn till såväl intresset av att förebygga brott som intresset av att utreda och lagföra framtida brott. Det bör därför räcka att en plats kan betraktas som brottsutsatt för att detta förhållande ska beaktas särskilt vid tillståndsprövningen. Regeringen framhöll även att kamerabevakningslagen bör innehålla bestämmelser om vilka särskilda hänsyn som ska tas vid tillståndsprövningen eftersom detta är en nödvändig förutsättning för en enhetlig och ändamålsenlig rättstillämpning på området. Vad som är en laglig och rättvis behandling av personuppgifter avgörs dock i slutändan genom en tillämpning av regleringen i de olika dataskyddsregleringarna. Detta innebär att

tillståndsprövningen inom dataskyddsdirektivets tillämpningsområde primärt ska utgå från en bedömning av om kamerabevakningen är förenlig med regleringen i brottsdatalagen eller annan personuppgiftsreglering som genomför dataskyddsdirektivet. Regeringen underströk även att kamerabevakning många gånger bör betraktas som ett naturligt hjälpmedel och som ett komplement till andra åtgärder. Detta innebär att andra åtgärder inte nödvändigtvis måste prövas innan kamerabevakning tillåts. (Se a. prop. s. 64 ff., 73 och 142 f.)

6.3 Personuppgiftsbehandling

När en bevakningskamera fångar en person på bild, på ett sätt som gör att personen kan identifieras, är det fråga om personuppgiftsbehandling. Begreppet personuppgifter innefattar varje upplysning som avser en identifierad eller identifierbar fysisk person som är i livet. Detta framgår bl.a. av 1 kap. 6 § brottsdatalagen. En identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare, såsom ett namn eller en annan uppgift som kan härledas till en persons identitet. För att en fysisk person ska anses vara identifierad krävs alltså inte att hans eller hennes fullständiga legala identitet, i form av t.ex. namn eller personnummer, kan fastställas. Det är tillräckligt att personen kan individualiseras och med tillräcklig säkerhet kännas igen. (Jfr t.ex. skäl 21 och artikel 3.1 dataskyddsdirektivet. Se också prop. 2017/18:232 s. 88.)

En uppgift som kan härledas till en fysisk person först efter att ha sammanförts med annan information eller genom användning av andra hjälpmedel är också en personuppgift. Det innebär t.ex. att ett fordons registreringsnummer som samlats in genom kamerabevakning under vissa förhållanden kan vara att anse som en personuppgift, om en fysisk person är registrerad ägare till fordonet. Detta eftersom identiteten på fordonets ägare enkelt kan tas fram genom uppgifter i vägtrafikregister. Om ett fordon kan knytas till en identifierad person med hjälp av registreringsnumret kan även annan information om denne framkomma genom att fordonsuppgifterna sammanförs med andra uppgifter. Exempelvis kan en uppgift om tid och plats för när ett fordon passerat en viss

kamerapunkt ge information om en fysisk persons rörelser eller resvanor, vilket också utgör en personuppgift. Registreringsnummer bör därför i vart fall som utgångspunkt betraktas som personuppgifter, trots att fordon också kan stå registrerade på juridiska personer vilka inte skyddas av personuppgifts- och dataskyddsregleringen (jfr resonemanget i SOU 2021:92 s. 386).

För att få behandla personuppgifter krävs att det bl.a. finns en rättslig grund och ett konkret ändamål (se bl.a. prop. 2018/19:147 s. 11 f.). Kamerabevakningslagen reglerar särskilt den personuppgiftsbehandling som sker vid kamerabevakning. Bestämmelserna i lagen kompletterar dataskyddsförordningen och genomför dataskyddsdirektivet, men lagen innehåller även bestämmelser som inte omfattas av dataskyddsförordningen och dataskyddsdirektivet (1 § kamerabevakningslagen). När en viss fråga inte är reglerad i kamerabevakningslagen gäller alltså de allmänna bestämmelserna i dataskyddsförordningen eller dataskyddsdirektivet med anslutande föreskrifter i andra författningar. Detta kan uttryckas som att kamerabevakningslagen preciserar och kompletterar den allmänna dataskyddsrättsliga lagstiftningen men, till skillnad från den tidigare kameraövervakningslagen (2013:460), inte gäller i stället för den allmänna dataskyddsregleringen.

Vid kamerabevakning avgör syftet med bevakningen vilka regler som är tillämpliga på personuppgiftsbehandlingen. Enligt 2 kap. 1 § brottsdatalagen finns det rättslig grund för behandling av personuppgifter bl.a. om behandlingen är nödvändig för att behöriga myndigheter ska kunna utföra sina uppgifter att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller upprätthålla allmän ordning och säkerhet. Särskilda bestämmelser om rättslig grund finns även i bl.a. säkerhetspolisens datalag.

När myndigheterna bedriver kamerabevakning för andra ändamål än inom brottsbekämpningen, exempelvis vissa former av kontroll eller tillsyn, gäller i regel dataskyddsförordningen och dataskyddslagen med anslutande föreskrifter. Om kamerabevakningen inte är nödvändig för de syften som anges i dessa regelverk är bevakningen över huvud taget inte tillåten (SOU 2021:92 s. 302).

6.4 Kamerabevakning med ANPR-teknik

Automatic number plate recognition (ANPR), eller automatisk igenkänning av registreringsskyltar, är ett samlingsbegrepp för system som använder sig av maskinläsning för att automatiskt läsa av fordons registreringsskyltar. Det är ett tekniskt verktyg för bildanalys, som används tillsammans med en kamera som fotograferar ett fordon. Ett ANPR-system består av en eller flera kameror som, tillsammans med en mjukvara kan urskilja och tolka registreringsskyltar på fordon. Därutöver brukar tid och plats för ett fordons passage registreras av systemet. Beroende på hur kameran ställs in kan även andra fordonsspecifika kännetecken utöver registreringsnummer registreras av systemet, t.ex. uppgifter om fordonstyp, fordonsmodell eller färg. Därutöver kan ofta ett fordons registreringsland gå att utläsa av registreringsskylten, eftersom det där ofta finns en nationalitetsbeteckning. Precis som bevakningskameror i allmänhet kan en kamera som utrustas med ANPR-teknik användas så att den även samlar in bild på förare eller passagerare i fordonet. För närvarande används inte ANPR-tekniken på det sättet av svenska brottsbekämpande myndigheter.

Sedan år 2015 använder bl.a. Polismyndigheten ANPR-teknik i polisbilar i syfte att beivra vissa trafikbrott. Denna användning av ANPR-teknik går till på följande sätt. Transportstyrelsen skickar information till Polismyndigheten om fordon som har olika identifierade ”brister”. Det kan t.ex. röra sig om att fordonet har körförbud, saknar försäkring, är avställt eller rapporterat stulet. Denna information bearbetas därefter av Polismyndigheten till särskilda s.k. bevakningslistor, som lagras i en central databas. När en polis-patrull loggar in i polisbilens ANPR-system laddas bevakningarna från databasen automatiskt ned i en lokal dator i polisbilen. Informationen används sedan genom att kameror i bilen automatiskt läser av mötande och framförvarande fordons registreringsskyltar. När ANPR-systemet upptäcker en registreringsskylt som förekommer i en bevakningslista notifieras patrullen om att det aktuella fordonet har en brist. Notifieringen sker endast lokalt i den polisbil som upptäckt fordonet, och den patrull som framför polisbilen kan därefter vidta lämpliga åtgärder. Utöver användning av ANPR-teknik i polisbilar pågår inom Polismyndigheten ett arbete med att bygga upp ett system för fast

kamerabevakning med ANPR-teknik i s.k. gränsnära områden enligt lagen (2023:474) om polisiära befogenheter i gränsnära områden. Lagen trädde i kraft den 1 augusti 2023. Tullverket använder redan i dag fasta kameror med ANPR-teknik i sin verksamhet (se avsnitt 6.5.4).

Kamerabevakningslagen är tillämplig på sådan kamerabevakning som beskrivs i 3 och 4 §§. Av 3 § framgår bl.a. att med kamerabevakning avses sådan bevakning som sker med kameror som används ”utan att manövreras på platsen”. Med att en kamera manövreras på platsen avses att den inte fortlöpande hanteras från en plats som är klart åtskild från den där kameran är uppsatt. Detta innebär bl.a. att lagen inte är tillämplig på handhållna kameror (prop. 2017/18:231 s. 40). Kamerabevakning som sker genom rörliga kameror i vindrutan på en polisbil omfattas inte av kamerabevakningslagens tillämpningsområde så länge någon framför polisbilen. Eftersom föraren i en sådan situation startar och stänger av kameran, samt avgör vad som ska filmas genom att styra fordonet, anses kameran vara manövrerad på platsen. (Se HFD 2016 ref. 71 [II].) Det torde sannolikt vara möjligt att anse att en kamera som på detta sätt är fäst i vindrutan på en polisbil är manövrerad på platsen även om de poliser som kör polisbilen helt tillfälligtvis och kortvarigt, t.ex. inom ramen för ett ingripande, avlägsnar sig från bilen, i vart fall så länge de inte avlägsnar sig någon längre sträcka från den. (Jfr Integritetsskyddsmyndighetens yttrande den 16 december 2021 Förhandssamråd enligt brottsdatalagen – kameror på och i polisfordon, dnr DI-2021-8344.)

För kamerabevakning som sker med fasta kameror är huvudregeln att kamerabevakningslagen gäller. Av bestämmelsen i 8 § kamerabevakningslagen följer att Polismyndigheten och Säkerhetspolisen som huvudregel ska göra en dokumenterad intresseavvägning före kamerabevakning inleds. Vid bedömningen ska faktorer som framgår av paragrafens andra och tredje stycken beaktas. Vid vissa situationer gäller dock inte kravet på att en dokumenterad intresseavvägning måste göras (se 14 c § kamerabevakningslagen).

En kamera som är utrustad med ANPR-teknik kan användas för att samla in vad som enligt dataskyddsdirektivet och brottsdatalagen är att betrakta som personuppgifter. Oavsett om kamerabevakning sker med fasta eller rörliga kameror måste kamerabevakning med

ANPR-teknik alltså ske i enlighet med tillämpliga dataskyddsrättsliga regler. Det innebär bl.a. att det måste finnas en rättslig grund och ett konkret ändamål med insamlingen och bearbetningen. Det ska även göras en bedömning av i vilken omfattning behandlingen är nödvändig och proportionerlig i förhållande till de personuppgifter som kan förväntas samlas in av kameran och därmed beröras av eventuell efterföljande behandling.

I samband med att undantaget om kamerabevakning i s.k. gränsnära områden infördes i kamerabevakningslagen infördes även en specialreglering i 13 § lagen (2023:474) om polisiära befogenheter i gränsnära områden avseende behandling av personuppgifter som rör fordon som har samlats in genom kamerabevakning i sådana områden. Dessa personuppgifter får alltid behandlas av Polismyndigheten och Säkerhetspolisen i sex månader efter det att uppgifterna samlats in, om syftet med behandlingen är att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. Detta gäller dock inte för personuppgifter i form av bilder av enskilda. Bestämmelsen avser bl.a. att möjliggöra att ANPR-teknik ska kunna användas i större utsträckning i gränsnära områden.

6.5 Kamerabevakning i vissa myndigheters verksamhet

6.5.1 Polismyndigheten

Polismyndigheten har i uppdrag att bl.a. förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten, övervaka den allmänna ordningen och säkerheten och ingripa när störningar har inträffat, utreda och beivra brott som hör under allmänt åtal. Polisens arbete ska syfta till att upprätthålla allmän ordning och säkerhet samt att i övrigt tillförsäkra allmänheten skydd och annan hjälp (se 1 och 2 §§ polislagen [1984:387]).

För att fullgöra sitt uppdrag bedriver Polismyndigheten bl.a. kamerabevakning på ett antal allmänna platser i landet med både fasta, tillfälliga och mobila kameralösningar som exempelvis drönare. Det kan röra sig om kontinuerlig bevakning av vissa gator och torg men också tillfällig bevakning i samband med

demonstrationer, festivaler, fotbollsmatcher och andra evenemang. Syftet med bevakningen är att upprätthålla allmän ordning och säkerhet, förebygga, förhindra eller upptäcka brottslig verksamhet på platsen och att i efterhand kunna utreda eller lagföra brott. Kamerorna ger också polisen bättre förutsättningar att effektivt leda och fördela sina resurser och kan bidra till att öka tryggheten i samhället. (Se SOU 2021:92 s. 196.)

Kamerateknik används även som ett verktyg i polisbilar. Det är då bl.a. fråga om kameror med ANPR-teknik som läser av registreringsnummer på passerande fordon och jämför informationen mot ett antal register.

Poliser i yttre tjänst i vissa regioner har i dag kroppskameror som kan spela in bild och ljud. Kamerorna kan bidra till att minska våld och hot mot polisen samt öka tryggheten för de personer som blir föremål för ett ingripande. Dessutom kamerabevakas flera av Polismyndighetens lokaler. (Se a. SOU s. 196 f.)

En stor del av Polismyndighetens kameramaterial lagras i myndighetens nationella kameraplattform. Allt bildmaterial lagras emellertid inte. Avsikten med kameraplattformen är att den ska vara utformad i enlighet med de grundläggande principer som ska genomsyra all personuppgiftsbehandling, däribland inbyggt dataskydd, krav på loggning och skydd mot att obehöriga får tillgång till uppgifterna. För att ta del av bildmaterialet i kameraplattformen krävs en personlig behörighet som tilldelas efter särskild ansökan. Innan en anställd vid Polismyndigheten får tilldelas behörighet till kameraplattformen ska han eller hon ha tagit del av myndighetens riktlinjer för användning av kameraplattsformen och genomgått en särskild utbildning med godkänt resultat. Det finns bl.a. en särskilt framtagen utbildning för kroppsburna kameror.

Behörigheten för åtkomst till kameraplattformen skiljer sig åt beroende på behov. Anställda i yttre tjänst har typiskt sett tillgång till bildmaterial från ett begränsat antal fasta och tillfälligt uppsatta kameror i sin region i realtid, inklusive ett begränsat inspelat material. Andra, exempelvis utredare, har enbart tillgång till inspelat material i viss omfattning. Vad gäller kroppsburna kameror har den enskilde polisen enbart behörighet till sitt eget inspelade material som överförts till kameraplattformen under en begränsad tid i enlighet med gällande riktlinjer. Behörigheten kan begränsas genom att enbart omfatta stationär åtkomst, men inte s.k. ”mobil access”.

Vid mobil access har den anställde tillgång till det material som omfattas av den anställdes behörighet via sin mobiltelefon eller dylikt. Behovet av mobil access finns bl.a. för personal i yttre tjänst som behöver kunna se vad som händer på en viss plats men som inte har tillgång till sin dator under arbetspasset. Utöver det ovanstående har endast särskilt utsedd personal behörighet att exportera material från kameraplattformen. Sådan behörighet förutsätter att personalen har genomgått en särskild utbildning och ansökt om en särskild behörighet för det ändamålet.

6.5.2 Trafikverket

Trafikverket är ansvarig myndighet för den statliga väghållningen (5 och 6 §§ väglagen [1971:948]). Med utgångspunkt i ett trafikslagsövergripande perspektiv ska Trafikverket ansvara för den långsiktiga infrastrukturplaneringen för vägtrafik, järnvägstrafik, sjöfart och luftfart samt för byggande och drift av statliga vägar och järnvägar (1 § förordningen [2010:185] med instruktion för Trafikverket).

Trafikverket har cirka 6 500 kameror runt om i Sverige. Kamerorna finns bl.a. vid vägar, järnvägar och färjelägen. Vissa av kamerorna är påslagna hela tiden medan andra endast är påslagna vissa förinställda tider beroende på bevakningens syfte. Kamerorna används bl.a. för att kontrollera fordons hastighet, läsa av väglaget, ge information om situationen i trafiken, hantera broöppningar och ge underlag till exempelvis Transportstyrelsen för att kunna ta ut avgifter och skatter kopplade till vägtrafiken.

Av 9 § kamerabevakningslagen framgår att Trafikverket får bedriva kamerabevakning utan tillstånd, om bevakningen avser vägtrafik, sjötrafik vid en rörlig bro, en betalstation eller kontrollpunkt som avses i bilagorna till lagen (2004:629) om trängselskatt och som sker för att samla in uppgifter som behövs för att beslut om trängselskatt ska kunna fattas och för att kontrollera att sådan skatt betalas, eller en betalstation på allmän väg som används vid uttag av infrastrukturavgifter enligt lagen (2014:52) om infrastrukturavgifter på väg och som sker för att samla in uppgifter som behövs för att beslut om infrastrukturavgift ska kunna fattas och för att kontrollera att sådan avgift betalas.

Trafikverket bedriver kamerabevakning på järnvägsplattformar och dess anslutningar, såsom exempelvis under- och övergångar, rulltrappor och trappor. I de fall kommunen förvaltar järnvägsplattformarnas anslutningar bedriver Trafikverket ingen kamerabevakning. Trafikverket kamerabevakar inte heller stationshus eftersom myndigheten inte förvaltar dessa. De flesta av Trafikverkets kameror på järnvägsplattformar ger en detaljerad bild för identifikation. Syftet med kamerabevakningen kan vara flera. Det kan bl.a. handla om att bekämpa brott, förebygga olyckor eller ge underlag för behov av underhåll av plattformarna. Sedan tillståndskravet i kamerabevakningslagen togs bort för Trafikverkets kamerabevakning bygger myndigheten sin kamerabevakning så att den alltid kan identifiera personer vid något tillfälle när de anländer på plattformen eller vid över- och undergångar, både som avresande och ankommande. Materialet från kameror vid järnvägsplattformar sparas i sju dagar. Alla kameror på järnvägsplattformar hanterar strömmande bilder.

Trafikverket bedriver även kamerabevakning på vissa färjor och vid vissa färjelägen. Syftet med kamerabevakningen är lastplanering. Dessa kameror spelar inte in något material.

I vägtrafiken bedriver Trafikverket olika typer av kamerabevakning, bl.a. i tunnlar, på vägars ytskikt, vid betalstationer och kontrollpunkter för trängselskatt och infrastrukturavgifter samt på olycksdrabbade vägar i form av trafiksäkerhetskameror. Kamerorna som bevakar vägytan och i tunnlar visar en översiktsbild av trafikläget och registrerar vanligen inte uppgifter om enskilda personer eller registreringsskyltar. Dessa kameror hanterar strömmande bilder men alla spelar inte in och något material lagras då inte.

Verksamheten med trafiksäkerhetskameror bygger på ett samarbete mellan Trafikverket och Polismyndigheten. Det gemensamma uppdraget är att öka trafiksäkerheten längs vägarna. Vid årsskiftet 2023/24 fanns det omkring 2 500 trafiksäkerhetskameror. Kamerorna mäter fordonets hastighet med hjälp av radar och fotograferar bara när någon kör fortare än vad som är tillåtet på vägen. Fotograferingen sker av aktuellt fordons registreringsskyltar och förarens ansikte. Kamerorna är placerade utmed det statliga vägnätet. (Se www.trafikverket.se.) Trafiksäkerhetskamerorna kan vara fast placerade vid vägkanten eller monterade i en släpvagn. Trafikverket ansvarar för de fasta kamerorna och Polismyndigheten för de

mobila. Myndigheterna är gemensamt ansvariga för hur och i vilken omfattning trafiksäkerhetskamerorna ska användas.

Kameror som är uppställda för att kunna ta ut trängselskatt och infrastrukturavgift genererar stillbilder som innehåller information om passerande fordons registreringsskylt, fram och bak, samt tid och plats för passagen. Bilderna skickas till Transportstyrelsen som använder bilderna för att kunna fullgöra sitt uppdrag om avgifts- och skattebeläggning. Vid ett omprövningsärende får även Skatteverket del av bilderna.

Som framgått ovan är det inte alla kameror som genererar strömmande bilder som spelar in material. De kameror som spelar in ger olika typer av material. Vissa kameror genererar bilder som ger detaljerad information och innehåller bl.a. personuppgifter medan andra enbart ger en översiktsbild av trafikläget. Stillbilder från olika kameror sparas i vart fall under en tid. Material från Trafikverkets kameror delas på olika sätt med andra myndigheter när det behövs för att fullgöra olika lagstadgade uppdrag (se avsnitt 8).

6.5.3 Transportstyrelsen

Transportstyrelsen är bl.a. ansvarig för att besluta om och kräva in infrastrukturavgift för Trafikverkets räkning och trängselskatt för Skatteverkets räkning (se 3 § andra stycket förordningen [2014:1564] om infrastrukturavgifter på väg och 2 § andra stycket lagen [2004:629] om trängselskatt).

Infrastrukturavgift tas ut för fordon som passerar Motalabron, Sundsvallsbron och Skurubron (se 4 § förordningen (2014:1564) om infrastrukturavgifter på väg). Som framgått ovan under avsnitt 6.5.2 ansvarar Trafikverket för kamerorna vid betalstationerna vid broarna. Dessa tar bild av passerande fordons registreringsskyltar. Det finns även information om tid och plats för passagen. Kamerorna är påslagna dygnet runt.

Trängselskatt tas ut vid vissa tider för fordon som passerar betalstationer i Göteborgs och Stockholms kommun. Fordonen registreras av kameror vid betalstationerna som tar bild av passerande fordons registreringsskyltar. I Göteborg finns, för visst ändamål, också s.k. kontrollpunkter, där bilar också registreras med

kameror. Trafikverket ansvarar även för kamerorna vid betalstationer och kontrollpunkter för trängselskatt.

För att kunna fullgöra sitt uppdrag om avgifts- och skattebeläggning får Transportstyrelsen ta del av bilder från Trafikverkets kameror som är uppsatta för dessa syften. Bilderna skickas elektroniskt till Transportstyrelsen som en sammanställning om 5 000 passager per gång vid flera tillfällen under ett dygn eller var femte minut. Det sistnämnda är framför allt aktuellt nattetid för material från kameror på ovannämnda broar, då det vid denna tid på dygnet inte passerar särskilt många fordon och det annars skulle ta lång tid innan Transportstyrelsen fick en ny sammanställning av bilder.

6.5.4 Tullverket

Tullverket ansvarar bl.a. för att fastställa och ta ut tullar, skatter och avgifter så att en riktig uppbörd kan säkerställas, övervaka och kontrollera trafiken till och från Sverige så att bestämmelser om in- och utförsel av varor följs, förebygga och motverka brottslighet i samband med in- och utförsel av varor, bedriva viss utrednings- och åklagarverksamhet i fråga om brott mot bestämmelser om in- och utförsel av varor samt bedriva viss verksamhet i fråga om rattfylleribrott (se 1–5 §§ förordningen [2016:1332] med instruktion för Tullverket).

Tullverket bedriver kamerabevakning vid gränspassager. Kamerorna är påslagna alla dagar i veckan, dygnet runt och genererar en kort kamerasekvens av passerande fordons registreringsskylt. Tullverket använder sig bl.a. av ANPR-teknik i sin verksamhet. ANPR-tekniken är ett komplement till tulltjänstemännens verktyg för urval och selektering av vilka fordon som ska tas ut för tullkontroll. När ANPR-tekniken har läst av en registreringsskylt stäms denna uppgift av mot Tullverkets underrättelseuppgifter. Detta sker genom ett automatiskt förlopp via en mjukvara. Om det blir en träff sker en selektering och uppgiften går då till en handläggare på Tullverket som kontrollerar aktuellt fordon.

Tullverket är en av de myndigheter som enligt 14 c § kamerabevakningslagen kan bedriva kamerabevakning utan tillstånd och utan att göra en dokumenterad intresseavvägning, om det sker i

gränsnära områden som avses i 2 § lagen (2023:474) om polisiära befogenheter i gränsnära områden eller av tillfartsvägar till sådana gränsnära områden som avses i 2 § 3 eller 4 samma lag, om bevakningen bedrivs inom 20 kilometer från området. Detta undantag tillkom samtidigt som lagen om polisiära befogenheter i gränsnära områden och motiverades bl.a. av att gränsen och de gränsnära områdena är områden som är av avgörande vikt i arbetet med att bekämpa den gränsöverskridande brottsligheten (prop. 2022/23:109 s. 34 f.). Som gränsnära områden definieras enligt 2 § lagen (2023:474) om polisiära befogenheter i gränsnära områden flygplatser och hamnar som har direktförbindelse med utlandet för kommersiell gods- eller passagerartrafik, järnvägsstationer som har direkt förbindelse med utlandet för kommersiell passagerartrafik, broar för vägtrafik till eller från utlandet och gränsövergångsställen på allmänna vägar.

I dagsläget sparas inte bilderna från Tullverkets kameror, men myndigheten kommer i detta avseende att anpassa sitt arbetssätt för att utnyttja det lagliga utrymme som ges i 13 § lagen om polisiära befogenheter i gränsnära områden. Av den bestämmelsen framgår att personuppgifter som rör fordon och som har samlats in genom kamerabevakning i ett gränsnära område alltid får behandlas av Polismyndigheten, Säkerhetspolisen eller Tullverket i sex månader efter det att uppgifterna samlades in, om syftet med behandlingen är att förebygga, förhindra eller upptäcka brottslig verksamhet eller att utreda eller lagföra brott. Detta gäller dock inte för personuppgifter i form av bilder av enskilda.

När Tullverket i egenskap av behörig myndighet behandlar personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller att utreda eller lagföra brott gäller, utöver brottsdatalagen, även lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område. Det har upplysts att Tullverket kommer att installera ytterligare kameror vid gränspassager än de som finns i dagsläget.

7 Rättsliga förutsättningar för Polismyndigheten och Säkerhetspolisen att ta del av material från andra aktörers bevakningskameror

7.1 Inledning

I Sverige bedrivs polisverksamhet av Polismyndigheten och Säkerhetspolisen. Till Polismyndighetens uppgifter hör bl.a. att förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten, övervaka den allmänna ordningen och säkerheten och ingripa när störningar har inträffat samt utreda och beivra brott som hör under allmänt åtal. Polisens arbete ska således syfta till att upprätthålla allmän ordning och säkerhet samt att i övrigt tillförsäkra allmänheten skydd och annan hjälp. (Se 1 och 2 §§ polislagen [1984:387].)

Till Säkerhetspolisens uppdrag hör bl.a. att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott samt att utreda och beivra bl.a. sådana brott. När Säkerhetspolisen leder polisverksamhet ska det som i lag eller annan författning föreskrivs om Polismyndigheten i tillämpliga delar gälla Säkerhetspolisen (se 3 § polislagen).

Polismyndigheten och Säkerhetspolisen har möjlighet att enligt bl.a. kamerabevakningslagen (2018:1200) bedriva kamerabevakning på egen hand för att fullgöra sina uppdrag. Myndigheterna är dock ofta behjälpta av att få ta del av material från andra aktörers bevakningskameror.

I detta avsnitt redogörs för de möjligheter Polismyndigheten och Säkerhetspolisen har, enligt gällande rätt, att få tillgång till material

från andra aktörers bevakningskameror. Det avsedda materialet är sådant som Polismyndigheten och Säkerhetspolisen behöver i sin brottsutredande eller brottspreventiva verksamhet. I avsnittet behandlas frågan om tillgång till material från bevakningskameror som ägs av enskilda aktörer och andra myndigheter.

7.2 Utlämnande av material från bevakningskameror med stöd av straffprocessuella tvångsmedel, m.m.

Polismyndigheten och Säkerhetspolisen har möjlighet att få del av material från andra aktörers bevakningskameror med tillämpning av lagstiftningen om straffprocessuella tvångsmedel och vissa andra bestämmelser i rättegångsbalken.

I 27 kap. RB finns bestämmelser om bl.a. bevisbeslag. Enligt 27 kap. 1 § RB får polisen ta ett föremål i beslag om det bl.a. skäligen kan antas ha betydelse för utredning om brott, om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse, det vill säga om åtgärden är proportionerlig. Enligt andra stycket gäller kapitlets bestämmelser om föremål även i fråga om skriftlig handling, om inte annat sägs. Enligt 2 och 3 §§ i samma kapitel gäller strängare villkor för vissa typer av skriftliga handlingar.

Möjligheten att kopiera en handling som har blivit tillgänglig genom husrannsakan förutsätter inte att handlingen har tagits i beslag. Kopiering av fysiska handlingar och elektroniskt lagrad information regleras i 27 kap. 17 a § RB. Där föreskrivs att en handling som tagits i beslag eller påträffats vid en husrannsakan eller en genomsökning på distans får kopieras, bl.a. om den skäligen kan antas ha betydelse för utredning om brott. Av bestämmelsens andra stycke framgår att en handling som inte får tas i beslag enligt reglerna i 2 eller 3 § inte heller får kopieras. I 27 kap. 17 b–17 e §§ RB finns vissa kompletterande regler om tillvägagångssättet för kopiering av handlingar, bl.a. regler om vem som får besluta om kopiering.

En annan typ av straffprocessuellt tvångsmedel som kan komma i fråga att använda för att ge polisen tillgång till material från andra aktörers bevakningskameror är möjligheten att med tvång genom-

föra biometrisk autentisering, vilket regleras i 27 kap. 17 f § RB. Där föreskrivs att om det finns anledning att anta att någon har möjlighet att öppna ett avläsningsbart informationssystem genom biometrisk autentisering är han eller hon skyldig att på tillsägelse av en polis medverka till detta, om en genomsökning av ett beslagtaget föremål, en husrannsakan eller en genomsökning på distans annars försvåras. Om han eller hon vägrar, får en polis genomföra autentiseringen.

Med ett avläsningsbart informationssystem avses exempelvis en mobiltelefon, surfplatta eller dator. En biometrisk autentisering innebär att en elektronisk mätning görs av någons fysiska karaktärsdrag, t.ex. av fingeravtryck, näthinna eller ansiktsgeometri. (Se prop. 2021/22:119 s. 173.)

De brottsbekämpande myndigheterna kan under vissa förutsättningar besluta om husrannsakan för att söka efter föremål som kan tas i beslag (t.ex. sådana föremål som kan tas i bevisbeslag enligt 27 kap. 1 § RB). Detta framgår av 28 kap. 1 § RB.

I 38 kap. RB finns vidare regler om s.k. edition, det vill säga en förpliktelse för någon att tillhandahålla skriftliga handlingar. Av 38 kap. 2 och 4 §§ RB framgår att en domstol, på ansökan av en part i en rättegång, kan besluta om att en handling som har betydelse som bevis och som innehas av någon annan ska läggas fram. Om det kan antas att handlingen i fråga kommer att få betydelse som bevis för ett i målet aktuellt bevistema kan editionsplikten aktualiseras redan före rättegångens inledande. Den som är misstänkt i ett brottmål omfattas inte av skyldigheten att lägga fram skriftliga handlingar. En sådan skyldighet gäller inte heller för vissa personer som är närstående till den misstänkte. Bestämmelserna om edition är i allmänhet inte särskilt användbara för Polismyndigheten när det gäller att inhämta material från andra aktörers bevakningskameror under en förundersökning.

Det finns inget som hindrar att Polismyndigheten och Säkerhetspolisen begär att få in material från andra aktörers bevakningskameror utan tillämpning av tvångsmedelslagstiftningen. Under förutsättning att det är förenligt med dataskyddslagstiftningen och offentlighets- och sekretesslagen har Polismyndigheten och Säkerhetspolisen möjlighet att ta del av material från andra aktörers bevakningskameror på annat sätt.

7.3 Utlämnande av material från bevakningskameror med stöd av offentlighets- och sekretesslagen

Av 2 kap. 1 § TF framgår att var och en har rätt att ta del av allmänna handlingar. Bilder från bevakningskameror omfattas av uttrycket handlingar. Reglerna i 2 kap. TF gäller dock inte när myndigheter lämnar uppgifter till varandra. Om det saknas en författningsreglerad uppgiftsskyldighet omfattas en begäran från en myndighet som vill ta del av handlingar som finns hos en annan myndighet av 6 kap. 5 § OSL. Av bestämmelsen framgår att en myndighet på begäran av en annan myndighet ska lämna uppgift som den förfogar över, om inte uppgiften är sekretess-belagd eller det skulle hindra arbetets behöriga gång. Bestämmelsen anses utgöra en precisering av den allmänna samverkansskyldighet som gäller för myndigheter enligt 8 § förvaltningslagen (2017:900) och syftar bl.a. till att underlätta för myndigheter att fullgöra sin verksamhet. Skyldigheten enligt bestämmelsen är mer vidsträckt än den gentemot allmänheten och gäller varje uppgift som myndigheten förfogar över, det vill säga inte bara uppgifter ur allmänna handlingar. En längre gående uppgiftsskyldighet än den som framgår av bestämmelsen kan följa av särskilda föreskrifter (se bl.a. regleringen i ett flertal paragrafer i 10 kap. och bestämmelserna 25 kap. 12 § och 26 kap. 9 § OSL).

Vid utlämnande av allmänna handlingar gäller särskilda skyndsamhetskrav enligt 2 kap. TF. Eftersom 2 kap. TF inte är tillämpligt vid utbyte av information mellan myndigheter gäller det särskilda skyndsamhetskrav som stadgas i 2 kap. 15 § TF inte i en sådan situation (se HFD 2021 ref. 10). Något skyndsamhetskrav är inte uttryckligen reglerat när information lämnas enligt 6 kap. 5 § OSL. Dock framgår exempelvis av 5 kap. 3 a § vägtrafikdataförordningen att Transportstyrelsen på begäran av Polismyndigheten eller Säkerhetspolisen utan dröjsmål ska lämna ut sådana uppgifter som omfattas av bestämmelsen. Sist nämnda bestämmelse innehåller alltså ett särskilt skyndsamhetskrav.

Av 1 kap. 7 § dataskyddslagen kan utläsas att utlämnande av allmänna handlingar enligt 2 kap. TF undantas från dataskyddsregleringen. Eftersom reglerna i 2 kap. TF inte gäller när myndigheter lämnar uppgifter till varandra måste ett utlämnande av

personuppgifter från en myndighet till en annan vara förenlig med de grundläggande principerna i dataskyddsförordningen eller dataskyddsdirektivet (se HFD 2021 ref. 10).

7.3.1 Generellt om sekretess

Sekretess innebär ett förbud att röja en uppgift vare sig det sker muntligen, genom utlämnande av allmän handling eller på något annat sätt. Sekretess innebär alltså både en handlingssekretess och en tystnadsplikt (jfr 1 kap. 1 § andra stycket och 3 kap. 1 § OSL).

För att en handling ska omfattas av sekretess krävs som huvudregel att tre förutsättningar är uppfyllda. För det första ska handlingen innehålla uppgifter som omfattas av föremålet för sekretessen, det vill säga det ska vara fråga om sådana uppgifter som kan eller ska hemlighållas enligt aktuell bestämmelse. Det kan exempelvis vara uppgifter om enskildas personliga och ekonomiska förhållanden. För det andra ska uppgifterna i handlingen omfattas av bestämmelsens räckvidd. Detta bestäms normalt genom att det i bestämmelsen preciseras att sekretessen för de angivna uppgifterna endast gäller i en viss typ av ärende, i en viss typ av verksamhet eller hos en viss myndighet. Vanligtvis ska även en bedömning göras om vilken effekt ett röjande av uppgifter i handlingen får för en eller flera personer. Detta bestäms av ett s.k. skaderekvisit. Det finns olika typer av skaderekvisit. Exempelvis skiljer man mellan raka och omvända skaderekvisit.

Ett *rakt skaderekvisit* föreskriver att sekretess ska gälla för en viss typ av uppgift ”om det kan antas” att exempelvis den enskilde lider men eller skada om uppgiften röjs.[13] Vid ett rakt skaderekvisit är utgångspunkten att uppgifterna är offentliga. En del bestämmelser innehåller ett *rakt kvalificerat skaderekvisit*, vilka föreskriver att sekretess ska gälla för en viss typ av uppgift ”om det av särskild anledning kan antas” att exempelvis den enskilde lider men eller skada om uppgiften röjs.[14]

Ett *omvänt skaderekvisit* har den motsatta utgångspunkten, det vill säga att sekretess är huvudregel. Vid ett omvänt skaderekvisit

[13] Se exempelvis 31 kap. 17 § OSL.
[14] Se exempelvis 31 kap. 16 § OSL.

gäller sekretess, ”om det inte står klart” att uppgiften kan röjas utan att exempelvis den enskilde lider men eller skada.[15]

En bestämmelse kan även föreskriva om *absolut sekretess*. Det innebär att det i bestämmelsen saknas ett skaderekvisit. Uppgifter som omfattas av absolut sekretess ska hemlighållas utan att det ska göras en bedömning av vilken effekt ett utlämnande får.[16]

Sekretess gäller som huvudregel inte bara vid utlämnande av uppgifter ur handlingar i förhållande till enskilda utan också mellan myndigheter, eller inom en myndighet, om där finns olika verksamhetsgrenar som är att betrakta som självständiga i förhållande till varandra (8 kap. 1 och 2 §§ OSL).

En sekretessbestämmelse kan vara antingen primär eller sekundär. Definitionen av begreppen finns i 3 kap. 1 § OSL. Av bestämmelsen framgår att en primär sekretessbestämmelse är en bestämmelse som ska tillämpas av en myndighet på grund av att bestämmelsen riktar sig direkt till myndigheten eller omfattar en viss verksamhetstyp eller en viss ärendetyp som hanteras hos myndigheten eller omfattar vissa uppgifter som finns hos myndigheten. En sekundär sekretessbestämmelse är en bestämmelse om sekretess som en myndighet ska tillämpa på grund av en bestämmelse om överföring av sekretess.

Om en myndighet får en uppgift överlämnad till sig från en annan myndighet har den mottagande myndigheten i normalfallet att pröva om uppgiften omfattas av sekretess utifrån de primära sekretessbestämmelserna, det vill säga de som gäller hos den mottagande myndigheten. Detta innebär att en uppgift som är skyddad av sekretess hos den överlämnande myndigheten kan ha ett svagare sekretesskydd eller rentav vara offentlig hos den mottagande myndigheten. Det finns dock bestämmelser om överföring av sekretess, som innebär att sekretessen följer med uppgiften när den lämnas till en annan myndighet eller verksamhet. Det är då en sekundär sekretessbestämmelse kan bli tillämplig. Bestämmelser om överföring av sekretess finns bl.a. i 43 kap. OSL. Av 43 kap. 2 § OSL framgår exempelvis att om en domstol i sin rättskipande eller rättsvårdande verksamhet får en sekretessreglerad uppgift från en domstol eller en annan myndighet, blir sekretessbestämmelsen, om

[15] Se exempelvis 26 kap. 1 § OSL.
[16] Se exempelvis 27 kap. 1 § OSL.

inte annat följer av 3 §, tillämplig på uppgiften även hos den mottagande domstolen.

Bestämmelser om överföring av sekretess finns även i bl.a. 11 kap. OSL. 11 kap. 4 § OSL reglerar sekretess vid direktåtkomst och stadgar att om en myndighet hos en annan myndighet har elektronisk tillgång till en upptagning för automatiserad behandling och en uppgift i denna upptagning är sekretessreglerad, blir sekretessbestämmelsen tillämplig även hos den mottagande myndigheten.

Om en uppgift är sekretessreglerad i flera bestämmelser och en sekretessprövning innebär att uppgiften kan lämnas ut enligt vissa av bestämmelserna samtidigt som den ska hemlighållas enligt en eller flera andra, är huvudregeln att de senare bestämmelserna ska ha företräde, om inte annat anges i lag. I ett sådant fall ska uppgiften hemlighållas (jfr 7 kap. 3 § OSL).

För att en uppgift ska få lämnas ut när den omfattas av sekretess krävs att en sekretessbrytande bestämmelse är tillämplig. Ett exempel på en sekretessbrytande bestämmelse är den i 10 kap. 28 § OSL, av vilken framgår att sekretess inte hindrar att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning.

Sekretessen begränsas ofta till en viss tid. Exempelvis framgår av 18 kap. 1 § tredje stycket OSL att sekretess för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott gäller i högst 40 år.

7.3.2 Sekretess för material från bevakningskameror

Möjligheterna att lämna ut material från bevakningskameror regleras i kamerabevakningslagen och offentlighets- och sekretesslagen. Av 22 § första stycket kamerabevakningslagen framgår att den som tar befattning med en uppgift som har inhämtats genom kamerabevakning inte obehörigen får röja eller utnyttja det som han eller hon på detta sätt har fått veta om någon enskilds personliga förhållanden. Bestämmelsen gäller både för offentliga och enskilda aktörer som bedriver kamerabevakning. Av paragrafens andra stycke framgår att i det allmännas verksamhet tillämpas offentlighets- och

sekretesslagen i stället för första stycket i 22 § kamerabevakningslagen. Obehörighetsrekvisitet i första stycket är avsett att tolkas på så sätt att ett uppgiftslämnande av en enskild aktör som motsvarar ett uppgiftslämnande som är tillåtet enligt offentlighets- och sekretesslagen inte är att betrakta som obehörigt. (Se prop. 2017/18:231 s. 157.) De bestämmelser i offentlighets- och sekretesslagen som är aktuella att tillämpa är 32 kap. 3 § och 32 kap. 3 a § OSL.

Av 32 kap. 3 § första stycket OSL framgår att sekretess gäller för uppgift om enskilds personliga förhållanden som har inhämtats genom kamerabevakning enligt kamerabevakningslagen, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. Vad som menas med personliga förhållanden ska bestämmas med ledning av vanligt språkbruk. Uttrycket avser så vitt skilda förhållanden som t.ex. en persons adress eller yttringarna av ett psykiskt sjukdomstillstånd (prop. 1979/80:2 Del A s. 84). Även uppgift om enskilds namn omfattas av begreppet (se RÅ 1994 not 516 och prop. 2003/04:93 s. 45).

Bestämmelsen i 32 kap. 3 § första stycket OSL innehåller ett omvänt skaderekvisit, vilket innebär en presumtion för sekretess. Som skäl för att ge sekretessen denna styrka anfördes i förarbetena att de uppgifter som samlas in genom kameraövervakning normalt är att betrakta som känsliga från ett integritetsperspektiv bl.a. då det med hjälp av sådana uppgifter är möjligt att kartlägga enskildas rörelsemönster (prop. 2012/13:115 s. 98 f.).

Bestämmelsens räckvidd har inte begränsats. Sekretessen är alltså tillämplig hos alla aktörer som själva inhämtar uppgifter med hjälp av bevakningskameror och hos myndigheter som får material från kamerabevakning överlämnat till sig. Detta gäller oavsett om materialet överlämnas från andra myndigheter eller från enskilda. (Se prop. 2012/13:115 s. 97 f.)

Uppgifter från en bevakningskamera kan i vissa fall även omfattas av annan sekretess än den som gäller enligt 32 kap. 3 § OSL. Som exempel kan nämnas att sekretessen enligt 25 kap. 1 § OSL är tillämplig även på uppgifter som har inhämtats vid patientövervakning med en bevakningskamera.

7.3.3 Sekretess för material från trängselskattekameror och infrastrukturavgiftskameror

En trängselskattekamera är en form av bevakningskamera. För material från trängselskattekameror gäller dock starkare sekretess än för material från andra bevakningskameror. Enligt 27 kap. 1 § första stycket OSL gäller absolut sekretess bl.a. för uppgift om en enskilds personliga eller ekonomiska förhållanden i en verksamhet som avser bestämmande av skatt. Någon prövning av vilken effekt ett utlämnande av uppgifter får ska alltså inte göras.

I 27 kap. 6 § OSL finns en bestämmelse om undantag från sekretess i skatteärenden. Av bestämmelsen följer dock att uppgift om vilken betalstation eller kontrollpunkt en bil har passerat och tidpunkten för passagen omfattas av sekretess även i ett beslut om trängselskatt och dess underlag. Eftersom den bestämmelse som ger den enskilde det starkaste sekretesskyddet har företräde om flera sekretessbestämmelser är tillämpliga samtidigt är det i första hand bestämmelserna om den absoluta skattesekretessen som tillämpas på uppgifterna om trängselskatt i vägtrafikregistret.

Av 29 kap. 5 a § första stycket OSL framgår att sekretess gäller i verksamhet som avser bestämmande av infrastrukturavgift på väg, avgift med anledning av att infrastrukturavgift inte har betalats i rätt tid, eller fastställande av underlag för bestämmande av sådana avgifter för uppgift om en enskilds personliga eller ekonomiska förhållanden. Av bestämmelsens andra stycke framgår att i beslut om sådana avgifter som avses i första stycket gäller sekretessen endast för uppgift om vilken betalstation bilen har passerat och tidpunkten för denna passage.

7.3.4 Sekretessbrytande bestämmelser

I 32 kap. 3 a § OSL finns en sekretessbrytande bestämmelse som gäller för material från bevakningskameror. Där föreskrivs bl.a. att sekretessen enligt 3 § inte hindrar att uppgift om en enskilds personliga förhållanden lämnas till en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Tullverket, Kustbevakningen eller Skatteverket, om uppgiften behövs för att utreda ett begånget brott för vilket fängelse är föreskrivet eller för att förebygga, förhindra

eller upptäcka brottslig verksamhet som innefattar brott för vilket fängelse är föreskrivet.

I många fall när Polismyndigheten eller Säkerhetspolisen vill ta del av sekretessbelagda uppgifter som en annan myndighet eller privat aktör har samlat in genom kamerabevakning kan uppgifterna lämnas ut med stöd av 32 kap. 3 a § OSL. I vissa fall kan dock materialet även omfattas av annan sekretess hos den utlämnande aktören än den som gäller enligt 32 kap. 3 § OSL. Som exempel kan nämnas att sekretessen enligt 25 kap. 1 § är tillämplig även på uppgifter som har inhämtats vid patientövervakning med en bevakningskamera. Detta innebär att uppgifterna då inte kan lämnas ut med stöd av 32 kap. 3 a § OSL. Polismyndigheten och Säkerhetspolisen kan även i vissa fall ha behov av kameramaterialet för andra syften än de som anges i 32 kap. 3 a § OSL. Bestämmelsen blir då inte tillämplig.

Uppgifter som har samlats in via kamerabevakning kan även lämnas ut med stöd av andra sekretessbrytande bestämmelser än de i 32 kap. 3 a § OSL. Ett exempel är bestämmelsen i 10 kap. 24 § OSL som i vissa fall möjliggör att en uppgift som angår en misstanke om ett begånget brott och som omfattas av sekretess i vissa fall kan lämnas ut till de brottsbekämpande myndigheterna. En förutsättning är dock att fängelse är föreskrivet för brottet och detta kan antas leda till någon annan påföljd än böter. Vid införandet av bestämmelsen konstaterades det att den ordning som tidigare gällde hade bidragit till att det rådde oklarhet om i vilka situationer en myndighet hade rätt att lämna ut uppgifter om misstänkta brott till en annan myndighet. Av den anledningen ansågs det angeläget att utforma en reglering som så enkelt som möjligt gör klart för myndigheter i vad mån de har rätt att eller rent av är skyldiga att lämna ut uppgifter om brott. (Se prop. 1983/84:142 s. 21.) Syftet med bestämmelsen var att ge samhället ökade möjligheter att upptäcka och bestraffa brott (a. prop. s 27).

Det finns även i vissa fall möjlighet att lämna ut uppgifter från kamerabevakning som omfattas av sekretess med stöd av generalklausulen i 10 kap. 27 § OSL. Av bestämmelsen framgår att en sekretessbelagd uppgift får lämnas till en myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda. Som framgår redan av

bestämmelsens ordalydelse har den ett mycket brett tillämpningsområde. Bestämmelsen kan bl.a. användas för att lämna ut uppgifter för att avvärja brott. Uppgifter kan lämnas till Polismyndigheten och Säkerhetspolisen utan samband med en förundersökning, t.ex. inom ramen för myndigheternas spaningsverksamhet (prop. 1983/84:142 s. 18 f.).

Möjligheten att dela uppgifter mellan myndigheter med stöd av generalklausulen får utnyttjas mer sparsamt och med större försiktighet om informationen inte är sekretesskyddad hos den mottagande myndigheten. Detta gäller särskilt i fråga om uppgifter som är hemliga med hänsyn till enskilds intressen (prop. 1979/80:2 Del A s. 77). Om en uppgift inte skyddas av sekretess hos den mottagande myndigheten kan risken för att skada ska uppkomma vara så stor att uppgiften inte bör lämnas ut (a. prop. s. 91). I förarbetena har särskilt framhållits att generalklausulen är tillämplig i fråga om lämnande av sekretessbelagda uppgifter till polis eller åklagare under förundersökning i brottmål (a. prop. s. 327).

En uppgift som omfattas av sekretess kan även lämnas ut till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Detta föreskrivs i 10 kap. 2 § OSL. Av förarbetena framgår att bestämmelsen ska tillämpas relativt restriktivt. Det är inte tillräckligt att myndighetens arbete blir mer effektivt för att utlämning ska kunna ske enligt bestämmelsen (prop. 1979/80:2 Del A s. 465). JO har i flera ärenden uttalat att bestämmelsen är avsedd för situationer av undantagskaraktär. (Se t.ex. JO 1982/83:JO1 s. 238, JO 1984/85:JO1 s. 265 och JO:s beslut den 9 september 2014, dnr 3032-2011.)

Enligt 5 kap. 3 a § vägtrafikdataförordningen (2019:382) ska Transportstyrelsen på begäran av Polismyndigheten utan dröjsmål lämna ut uppgifter om trängselskatt som gäller passager av en betalstation eller kontrollpunkt, om det av begäran framgår att uppgifterna i ett brådskande fall behövs för att förhindra eller på annat sätt ingripa mot en handling som kan utgöra terroristbrott enligt 4 § terroristbrottslagen (2022:666) eller försök, förberedelse eller stämpling till eller underlåtenhet att avslöja eller förhindra sådant brott.

Det ska även nämnas att det finns en sekretessbrytande bestämmelse i 5 kap. 14 § vägtrafikdataförordningen (2019:382), av

vilken framgår att Transportstyrelsen på begäran av bl.a. Polismyndigheten och Säkerhetspolisen ska lämna ut en personuppgift i vägtrafikregistret i form av en fotografisk bild av en enskild.

Pågående lagstiftningsarbete

Utredningen om förbättrade möjligheter att utbyta information med brottsbekämpande myndigheter överlämnade betänkandet *Ökat informationsflöde till brottsbekämpningen* (SOU 2023:69) till regeringen i oktober 2023. Det innehåller ett förslag till en ny lag om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna. Enligt förslaget ska en rad statliga myndigheter vara skyldiga att på eget initiativ och på begäran lämna en uppgift till en brottsbekämpande myndighet, om uppgiften kan antas behövas i den brottsbekämpande verksamheten. I betänkandet lämnas också förslag till en ändrad lydelse av bestämmelsen i 10 kap. 24 § OSL som innebär att förutsättningarna för sekretessgenombrott enligt paragrafen vidgas på så sätt att det inte längre ska finnas någon begränsning vad gäller straffvärdet för det brott som misstanken avser. Uppgifter ska också kunna lämnas även när det inte finns en identifierad person som är misstänkt för brottet. Därutöver lämnas ett förslag till ändring i 5 kap. 3 a § vägtrafikdataförordningen som innebär att uppgiftsskyldigheten ska gälla i fler brådskande fall än i dagsläget. Enligt förslaget ska Transportstyrelsen, på begäran av Polismyndigheten, Säkerhetspolisen eller Tullverket utan dröjsmål lämna ut uppgifter om trängselskatt som gäller passager av en betalstation eller kontrollpunkt, om det av begäran framgår att uppgifterna behövs i ett brådskande fall för att förebygga, förhindra, upptäcka eller utreda en handling som kan utgöra brott för vilket det i straffskalan ingår fängelse i ett år eller mer eller ett straffbart försök eller en straffbar förberedelse eller stämpling till eller underlåtenhet att avslöja eller förhindra sådant brott.

Det pågår även en utredning (Förbättrade möjligheter till informationsutbyte mellan myndigheter, Ju 2023:22) som bl.a. har i uppdrag att lämna förslag på en generell bestämmelse som gör det möjligt att på ett effektivt sätt lämna uppgifter som omfattas av sekretess till skydd för enskilda till en annan myndighet, såväl på

begäran som på eget initiativ. Utredningens förslag i den delen ska redovisas senast den 30 augusti 2024.

7.4 Dataskyddsrättsliga aspekter

7.4.1 Finalitetsprincipen

Grunddragen i den dataskyddsrättsliga lagstiftningen som reglerar brottsbekämpande myndigheters hantering av personuppgifter har beskrivits ovan i avsnitt 5. Där framgår bl.a. att artikel 4 i dataskyddsdirektivet stadgar att personuppgifter bara får samlas in för särskilda, uttryckligt angivna och berättigade ändamål, och att behandling av personuppgifter för något annat ändamål som anges i artikel 1.1 i direktivet än det för vilket uppgifterna samlades in är tillåten endast om den personuppgiftsansvarige har rätt att behandla personuppgifter för ett sådant ändamål och behandlingen är nödvändig och står i proportion till det nya ändamålet. I Sverige har dataskyddsdirektivet införts i nationell rätt genom brottsdatalagen, med kompletterande registerförfattningar.

Dataskyddsdirektivet är tillämpligt på behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder (artikel 1.1 och artikel 2). Utanför detta område är dataskyddsförordningen tillämplig. När andra aktörer än brottsbekämpande myndigheter behandlar personuppgifter är det alltså i regel inte dataskyddsdirektivet som är tillämpligt på behandlingen. Förutsättningarna för sådana aktörer att lämna ut material som innehåller personuppgifter till Polismyndigheten och Säkerhetspolisen regleras huvudsakligen av dataskyddsförordningen. De grundläggande principerna för personuppgiftsbehandling enligt dataskyddsförordningen motsvarar i stor utsträckning de som gäller enligt dataskyddsdirektivet.

I artikel 5 dataskyddsförordningen föreskrivs bl.a. att personuppgifter bara får samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Att personuppgifter inte senare får behandlas på ett sätt som är oförenligt med det ursprungliga ändamål för vilket de samlats in kallas ibland för finalitetsprincipen. Material

som innehåller personuppgifter får alltså som utgångspunkt bara lämnas ut till en annan myndighet om det är förenligt med finalitetsprincipen. I vissa registerförfattningar anges dock att personuppgifter endast får behandlas för vissa angivna ändamål. Vidarebehandling för andra ändamål är då inte tillåten. I sådana fall brukar det anges att finalitetsprincipen inte gäller (prop. 2017/18:171 s. 90). Det kan också föreligga en författningsreglerad uppgiftsskyldighet för en myndighet. Denna behöver då inte göra en bedömning av om utlämnandet av uppgifterna är förenlig med finalitetsprincipen, om detta tydligt har beaktats av lagstiftaren i regleringen om uppgiftsskyldigheten. En vidarebehandling, det vill säga ett utlämnande, av personuppgifter är därmed tillåten i sådana författningsreglerade situationer oavsett om det är förenligt med insamlingsändamålet eller inte (SOU 2023:69 s. 673).

Gällande informationsutbyte mellan myndigheter enligt 6 kap. 5 § OSL har Högsta förvaltningsdomstolen anfört att genom sekretessbestämmelser hindras myndigheter från att lämna bl.a. integritetskänsliga uppgifter till andra myndigheter. Härigenom får lagstiftaren anses ha tagit ställning till när ett uppgiftslämnande är oförenligt med det eller de ändamål för vilka uppgifterna samlades in. Utöver sekretessprövningen ska den personuppgiftsansvariga myndigheten således inte göra någon kontroll av förenligheten med finalitetsprincipen i samband med utlämnande av uppgifter enligt 6 kap. 5 § OSL (HFD 2021 ref. 10).

Av skäl 50 till dataskyddsförordningen framgår att behandling av personuppgifter för andra ändamål än de för vilka de ursprungligen samlades in endast bör vara tillåten när detta är förenligt med de ändamål för vilka personuppgifterna ursprungligen samlades in. I dessa fall krävs det inte någon annan separat rättslig grund än den med stöd av vilken insamling av personuppgifter medgavs. Det räcker med andra ord att hänföra sig till den rättsliga grund och de berättigade ändamål som förelegat vid den ursprungliga insamlingen för att vidarebehandla personuppgifterna. Den rättsliga grunden för behandling av personuppgifter som finns i unionsrätten eller i medlemsstaternas nationella rätt kan också utgöra en rättslig grund för ytterligare behandling. För att fastställa om ändamålet med den nya behandlingen är förenligt med det ändamål för vilket personuppgifterna ursprungligen samlades in bör den person-

uppgiftsansvarige, efter att ha uppfyllt alla krav vad beträffar den ursprungliga behandlingens lagenlighet, göra en bedömning av de omständigheter som framgår av artikel 6.4 i dataskyddsförordningen.

Av artikel 6.4 i förordningen framgår att det som ska beaktas vid denna bedömning är kopplingen mellan insamlingsändamålet och det nya ändamålet, personuppgifternas art, det sammanhang inom vilket personuppgifterna har samlats in, eventuella konsekvenser för registrerade av den planerade fortsatta behandlingen och förekomsten av lämpliga skyddsåtgärder, som t.ex. kryptering, hos den aktör som kommer att behandla personuppgifterna för det nya ändamålet.

Det framgår också av artikel 6.4 att behandling av personuppgifter för andra ändamål är tillåten om den grundar sig på den registrerades samtycke, på unionsrätten eller en medlemsstats nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda de mål som avses i artikel 23.1. I de flesta fall finns inget samtycke till vidarebehandling från den enskilda. Det kan dessutom uppstå problem om samtycket tas tillbaka. Ett av målen enligt artikel 23.1 är att förebygga, utreda eller lagföra brott. En medlemsstat kan med stöd av artikeln införa ett generellt undantag i nationell rätt som tillåter utlämnande av personuppgifter till brottsbekämpande myndigheter i ett brottsbekämpande syfte. Unionsrättslig grund för en aktör att dela personuppgifter med en brottsbekämpande myndighet, när myndigheten ska använda uppgifterna för annat ändamål än det ursprungliga, finns bl.a. i dataskyddsdirektivet.

Gällande utlämnande av personuppgifter som samlats in genom kamerabevakning finns en rättslig grund i svensk rätt i 22 § första stycket kamerabevakningslagen jämte 32 kap. 3 och 3 a §§ OSL. Vid införandet av kameraövervakningslagen, som gällde innan kamerabevakningslagen, uttalade regeringen att om ett utlämnande av personuppgifter är tillåtet enligt 32 kap. 3 a § OSL är det även förenligt med finalitetsprincipen (prop. 2012/13:115 s. 111). Någon särskild prövning i förhållande till finalitetsprincipen behöver alltså inte göras i de fall då ett utlämnande av personuppgifter kan ske med stöd av 32 kap. 3 a § OSL. (Se prop. 2017/18:231 s. 157.)

Om situationen däremot är sådan att 32 kap. 3 a § OSL inte är tillämplig, det vill säga om exempelvis Polismyndigheten eller Säkerhetspolisen behöver kameramaterialet för andra syften än brottsbekämpning, får i stället den överlämnande aktören göra en prövning av om det är förenligt med finalitetsprincipen att lämna ut materialet. Vid denna bedömning ska alla de faktorer som framgår av artikel 6.4 i dataskyddsförordningen beaktas.

Ett utlämnande av personuppgifter kan även ske med stöd av artikel 6.1 första stycket f dataskyddsförordningen. Denna bestämmelse innehåller en allmän intresseavvägning och föreskriver att personuppgiftsbehandling alltid är tillåten om den är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre.

Enligt artikel. 6.1 f andra stycket förordningen gäller första stycket inte för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter. Bestämmelsen kan dock utgöra en grund för behandling av personuppgifter när andra aktörer behandlar personuppgifter genom att lämna ut dem till exempelvis Polismyndigheten eller Säkerhetspolisen, för att myndigheterna ska kunna fullgöra sina uppgifter.

7.4.2 Särskilt om informationsskyldighet

Som huvudregel måste den personuppgiftsansvarige informera den berörda personen om den personuppgiftsbehandling som sker när personuppgifter vidarebehandlas genom att lämnas ut till någon annan. Detta framgår, såvitt gäller dataskyddsförordningens tillämpningsområde, av artiklarna 14.1–14.3. Informationsskyldigheten gäller så länge det inte finns något tillämpligt undantag från nämnda skyldighet (se artikel 14.5, som bl.a. tillåter att undantag införs i den nationella rätten för vissa ändamål).

Av 5 kap. 1 § dataskyddslagen framgår att bestämmelserna i dataskyddsförordningen om information och rätt att få tillgång till personuppgifter inte gäller sådana uppgifter som den personuppgiftsansvarige inte får lämna ut till den registrerade enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning. Om den personuppgiftsansvarige inte är en myndighet,

gäller undantaget i första stycket även för uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen. Gällande Polismyndighetens och Säkerhetspolisens verksamhet får en bedömning göras om det kan antas att syftet med de polisiära åtgärderna riskerar att motverkas eller den framtida verksamheten skadas om uppgifterna lämnas ut till den registrerade (jfr 18 kap. 1 och 2 §§ OSL). Det är ofta av stor vikt för Polismyndighetens och Säkerhetspolisens arbete att myndigheten kan ta del av uppgifter utan att den berörda personen får kännedom om detta.

Pågående lagstiftningsarbete

Utredningen om förbättrade möjligheter att utbyta information med brottsbekämpande myndigheter har i betänkandet *Ökat informationsflöde till brottsbekämpningen* (SOU 2023:69) lämnat ett förslag till ändring i dataskyddslagen, genom vilket en ny rättslig grund ska införas. Den föreslagna rättsliga grunden innebär en generell uttrycklig möjlighet för enskilda att behandla personuppgifter för att lämna sådana uppgifter till de brottsbekämpande myndigheterna när dessa myndigheter framställer en sådan begäran. Förslaget grundar sig på det utrymme som enligt artiklarna 6.4. och 23.1 d i dataskyddsförordningen finns att införa regler i den nationella rättsordningen för när det är tillåtet att behandla personuppgifter genom att lämna dem vidare. Någon generell sådan bestämmelse finns ännu inte i svensk rätt, även om det finns bestämmelser som gäller vissa särskilda typer av personuppgifter, bland dem uppgifter om enskilda som kommer från kamerabevakning (jfr 22 § kamerabevakningslagen och 32 kap. 3 och 3 a §§ OSL).

8 Hantering och användning av material från kamerabevakning i trafiken

8.1 Inledning

Myndigheter som exempelvis Polismyndigheten, Transportstyrelsen och Skatteverket har olika lagstadgade uppdrag för vilka de är i behov av uppgifter från kameror i trafiken som Trafikverket ansvarar för. Utlämning av uppgifter mellan myndigheter sker vanligen med stöd av olika bestämmelser i bl.a. offentlighets- och sekretesslagen (se avsnitt 7.3). I vissa fall sker utlämning av uppgifter genom direktåtkomst. Det kan bl.a. ske när en myndighet behöver materialet för att fullgöra ett lagstadgat uppdrag. Direktåtkomsten kan då vara reglerad i lag. I avsnittet redogörs för hur visst material från Trafikverkets kameror i trafiken hanteras och delas med Polismyndigheten, Transportstyrelsen och Skatteverket för att dessa myndigheter ska fullgöra olika lagstadgade uppdrag.

8.2 Material från trafiksäkerhetskameror

Polismyndigheten bedriver olika typer av kamerabevakning för att fullgöra sitt lagstadgade uppdrag att bl.a. förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten samt att utreda och beivra brott som hör under allmänt åtal (se 2 § polislagen [1984:387]). När det gäller uppdraget att utreda hastighetsöverträdelser i trafiken använder Polismyndigheten bl.a. material från trafiksäkerhetskameror. I dagsläget finns cirka 2 500 trafiksäkerhetskameror runt om i landet. De är placerade på vägar där trafiken håller hög medelhastighet, över

gällande hastighetsgräns, och där skaderisken bedöms som stor. Kamerorna innehåller en radar och är ett komplement till Polismyndighetens övriga trafikövervakning. De kan vara fast placerade vid vägkanten eller monterade i en släpvagn. De är alltid synligt placerade och väl skyltade.

Verksamheten med trafiksäkerhetskamerorna bygger på ett samarbete mellan Trafikverket och Polismyndigheten. Trafikverket och Polismyndigheten har ett gemensamt ansvar för att placera ut trafiksäkerhetskamerorna. Trafikverket ansvarar för etablering, drift och underhåll av de fasta kamerorna och Polismyndigheten hanterar de mobila trafiksäkerhetskamerorna. Polismyndigheten ansvarar för utredning av ärenden. Trafikverket och Polismyndigheten är gemensamt ansvariga för hur och i vilken omfattning kamerorna ska användas.

Kamerorna är inte påslagna hela tiden och när de inte är påslagna tas inga bilder. Om ett fordon registreras överskrida den högsta tillåtna hastigheten tar kameran bild på fordonets registreringsskylt och förarens ansikte. Kamerorna generar stillbilder. Dessa skickas krypterat från Trafikverket till Polismyndigheten. Trafikverket kan inte ta del av någon information från kamerorna och Trafikverket lagrar inte heller några bilder. Alla kameror är direktkopplade till Polismyndigheten. Polismyndigheten är personuppgiftsansvarig och Trafikverket personuppgiftsbiträde för materialet som kamerorna genererar. Trafikverket innehar endast materialet för teknisk lagring och materialet utgör därför allmänna handlingar endast hos Polismyndigheten (jfr 2 kap. 13 § TF).

8.3 Material från kameror vid betalstationer och kontrollpunkter för trängselskatt och infrastrukturavgift

8.3.1 Transportstyrelsen

Trafikverket ansvarar för kamerorna som finns uppsatta vid betalstationer och kontrollpunkter för infrastrukturavgift och trängselskatt. För att kunna fullgöra sitt uppdrag om avgifts- och skattebeläggning får Transportstyrelsen ta del av bilder från Trafikverkets kameror som är uppsatta för dessa syften. Kamerorna är inställda

och vinklade så att de endast tar bilder på ett fordons registreringsskyltar. Det händer att viss överskottsinformation fastnar på bilderna, såsom en större del av det aktuella fordonet. Det kan hända om kameran har tagit bild för tidigt eller för sent, eller har varit felkalibrerad så att den inte fotograferar rakt i körfältet. I normalfallet är det dock endast fordonets registreringsskyltar och en liten bit runt omkring skyltarna som framgår av en bild. Oftast går det inte av en bild att utröna vilket märke det är på ett fordon som har passerat kameran. Under den tid som trängselskatt inte tas ut är kamerorna som är uppsatta för dessa syften inte aktiva och tar därmed inte några bilder. Passagebilderna gallras automatiskt hos Trafikverket efter sju dygn. (Se SOU 2018:65 s. 215.)

När Transportstyrelsen mottagit bilderna av Trafikverket läses registreringsnumren av och information om fordon och fordonsägare hämtas från trafikregistret. Detta sker automatiskt av en programvara. Hela systemet gällande trängselskatt kallas hos Transportstyrelsen för NAT (nationell trängselskatt). Det är inom det systemet som bildinsamling och bearbetning av bildmaterialet sker. Med ledning av tidpunkten för passagen beräknas skatten eller avgiften och skatt- eller avgiftsskyldigheten fastställs. (Se a. SOU s. 216.)

Bearbetningen av materialet hos Transportstyrelsen kan ta olika lång tid, från ca 15 minuter upp till flera timmar. Om sammanställningen innehåller få passager går det fortare än om det rör sig om ett stort antal passager. Hur lång tid det tar för systemet att tolka bilderna är också beroende av bildernas kvalitet. Det händer att det automatiska systemet inte klarar av att identifiera ett registreringsnummer på vissa bilder. Dessa bilder sorteras då ut och hamnar i en kö för manuell bildgranskning av Transportstyrelsens handläggare. Transportstyrelsen uppskattar att detta sker med 20 procent av bilderna men vid exempelvis dålig väderlek kan siffran vara högre. Från det att en bild tas av en kamera till dess att den har hanterats och ett registreringsnummer har identifierats i den manuella granskningen kan det gå flera dagar, beroende på hur många bilder som ligger i kö för granskning. Det gränssnitt av systemet för trängselskatt som handläggarna arbetar i kallas för HSA-webben (Hantera Skatter och Avgifter). I HSA-webben är det möjligt att se passage-bilderna. (Se a. SOU s. 216.)

Trafikverket kan i dagsläget ta del av materialet från kamerorna i syfte att säkerställa leveransen, det vill säga att bilderna upprätthåller den kvalitet som överenskommits. Den tekniska bearbetning och lagring som därigenom genomförs hos Trafikverket sker dock endast under en kortare tid.

Trafikverket och Transportstyrelsen har gjort bedömningen att Trafikverket är personuppgiftsbiträde och Transportstyrelsen är personuppgiftsansvarig enligt dataskyddsförordningen vid överföringen av kameramaterialet. Eftersom både Trafikverket och Transportstyrelsen har tillgång till materialet bör det utgöra allmänna handlingar hos båda myndigheterna (jfr 2 kap. 6 § TF).

8.3.2 Skatteverket

Om någon begär omprövning av Transportstyrelsens beslut om trängselskatt ska Skatteverket ompröva beslutet (jfr 15 a § jämte 2 § lagen om trängselskatt). För att kunna fullgöra detta uppdrag får Skatteverket tillgång till materialet som Transportstyrelsen fått del av från Trafikverkets kameror. Informationsutbytet sker med stöd av 5 kap. 3 § vägtrafikdataförordningen (2019:382), som jämte 10 kap. 28 § OSL möjliggör att uppgifterna, som vanligtvis omfattas av sekretess enligt 27 kap. 1 § OSL, lämnas ut till Skatteverket. Skatteverket får tillgång till uppgifterna genom en avtalsreglerad direktåtkomst via en s.k. Citrix-lösning. Direktåtkomsten sker med stöd av 4 kap. 22 § vägtrafikdataförordningen som stadgar att Skatteverket kan ges direktåtkomst till elektroniska handlingar i ärenden som avser fordonsrelaterade skatter enligt lagen om trängselskatt. Direktåtkomsten avser andra gemensamt tillgängliga uppgifter än de som finns i vägtrafikregistret (vilka Skatteverket har tillgång till enligt andra bestämmelser).

Citrix-lösningen innebär att Skatteverket, genom en ingång till HSA-webben, får tillgång till det material från Trafikverkets kamera som Transportstyrelsen har lagt till grund för sitt beslut om trängselskatt. Direktåtkomsten omfattar inte material från Trafikverkets kameror i obearbetad form. Skatteverket får alltså inte tillgång till uppgifter som inte resulterat i ett beslut om trängselskatt och inte heller uppgifter som redan har gallrats hos Trafikverket, vilket sker efter sju dygn. Genom direktåtkomsten har Skatteverkets

handläggare möjlighet att söka på alla registreringsnummer, personnummer eller organisationsnummer som finns i systemet, men syftet med direktåtkomsten är att Skatteverket endast ska söka på det aktuella ärende som omprövningen avser. Skatteverkets handläggare har inte möjlighet att söka efter exempelvis vissa tidsintervall, datum eller platser. Eftersom det är fråga om en direktåtkomst utgör materialet allmänna handlingar både hos Skatteverket och Transportstyrelsen (se bl.a. SOU 2023:69 s. 684). Genom direktåtkomsten torde både Skatteverket och Transportstyrelsen vara att anse som personuppgiftsansvariga för uppgifterna.

9 Polismyndighetens tillgång till material från andras bevakningskameror

9.1 Inledning

Med undantag för regler i olika författningar om under vilka förutsättningar aktörer får ges direktåtkomst till bl.a. personuppgifter hos en myndighet[17], finns det inte några bestämmelser som uttryckligen reglerar formerna för informationsutbyte mellan myndigheter. Material från bevakningskameror delas mellan myndigheter bl.a. när det behövs för att uppfylla olika lagstadgade uppdrag. Utlämnandet sker elektroniskt på olika sätt. I avsnittet redogörs för olika former av elektroniskt informationsutbyte och de olika sätt som i dagsläget finns för Polismyndigheten att ta del av material från andras bevakningskameror.

9.2 Elektroniskt informationsutbyte

När myndigheter delar information med varandra är en allmän utgångspunkt att det är upp till den utlämnande myndigheten att bedöma, bl.a. med utgångspunkt i hur integritetskänsliga uppgifterna är, på vilket sätt uppgifterna bör överlämnas till den mottagande myndigheten. Utlämning av uppgifter ska alltid ske på ett ändamålsenligt sätt.

Utredningen om förbättrade möjligheter att utbyta information med brottsbekämpande myndigheter har i betänkandet *Ökat informationsflöde till brottsbekämpningen* (SOU 2023:69) identifierat

[17] För exempel på sådana bestämmelser om direktåtkomst, se 3 kap. 7 § och 5 kap. 10 och 17 §§ polisens brottsdatalag.

att det finns två former av elektronisk överföring av uppgifter mellan myndigheter: 1) direktåtkomst och 2) elektroniskt utlämnande på annat sätt än genom direktåtkomst.

Begreppet direktåtkomst definieras inte i lag eller någon annan författning. En myndighet som har direktåtkomst till en annan myndighets register eller databas kan på egen hand söka efter uppgifter i databasen. Den kan även hämta in information till sitt eget system och bearbeta den där. Den mottagande myndigheten, det vill säga den myndighet som har direktåtkomst, kan dock inte påverka innehållet i registret eller databasen. Den ansvariga myndigheten saknar kontroll över vilka uppgifter som lämnas ut via direktåtkomst. Handlingar blir därför allmänna hos den mottagande myndigheten redan i och med att de tillgängliggörs genom direktåtkomst. Det kan leda till överskottsinformation för den mottagande myndigheten. Direktåtkomst ökar även riskerna för intrång i den personliga integriteten. Detta eftersom uppgifter blir tillgängliga för fler än bara den utlämnande myndigheten. (Se SOU 2023:69 s. 683 f.)

Direktåtkomst kan bli aktuellt för uppgifter för vilka det inte gäller sekretess i förhållande till den mottagande myndigheten. I första hand gäller det således offentliga uppgifter. Direktåtkomst kan emellertid även bli aktuellt för uppgifter som visserligen omfattas av sekretess, men som också omfattas av en uppgiftsskyldighet enligt lag eller förordning till förmån för den myndighet som får direktåtkomst till de aktuella uppgifterna. I undantagsfall kan en myndighet även, enligt en prövning på förhand, ges direktåtkomst till uppgifter med stöd av generalklausulen i 10 kap. 27 § andra stycket offentlighets- och sekretesslagen (2009:400), som då medger ett rutinmässigt utlämnande till den som har direktåtkomst. (Se prop. 2007/08:160 s. 73 f.)

Direktåtkomst anses vara en utlämnandeform som innebär risker från integritetssynpunkt (jfr SOU 2023:69 s. 684). Om en myndighet väljer att lämna ut handlingar digitalt krävs att reglerna om dataskydd följs. Detta innebär bl.a. att den utlämnande myndigheten, det vill säga den personuppgiftsansvarige, ska säkerställa en lämplig säkerhetsnivå i förhållande till de risker som ett utlämnande kan medföra (jfr artikel 5.1 f och artikel 32 dataskyddsförordningen samt artikel 4.1 f och artikel 29 dataskyddsdirektivet).

Elektroniskt utlämnande av uppgifter på annat sätt än genom direktåtkomst kallas ibland för utlämnande på medium för automatiserad behandling. Ett utlämnande av uppgifter på annat sätt än genom direktåtkomst kan exempelvis ske genom att personuppgifter delas via e-post, med USB-minne eller genom filöverföring från ett IT-system till ett annat. Informationsutbytet kan även ske automatiskt, exempelvis genom en s.k. fråga-svarstjänst i en app. Det finns flera integritetsfördelar med denna form av utlämnande i förhållande till direktåtkomst. Risken för överskottsinformation hos den mottagande myndigheten minskar eftersom ingen annan information än den som faktiskt lämnas över till mottagaren kan betraktas som allmän handling hos denne. (Se SOU 2023:69 s. 683 f.)

Högsta förvaltningsdomstolen har i rättsfallet HFD 2015 ref. 61 uttalat att det som är avgörande för gränsdragningen mellan vad som utgör direktåtkomst respektive utlämnande på annat sätt är om den aktuella upptagningen kan anses förvarad hos den mottagande myndigheten enligt 2 kap. 6 § TF. Det väsentliga är därför om upptagningen är tillgänglig för myndigheten med tekniska hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas. Den tekniska utformningen av en myndighets system för utlämnande är därför av betydelse för frågan om ett utlämnande ska anses ske genom direktåtkomst eller på annat sätt.

I sammanhanget kan nämnas bestämmelsen i 2 kap. 13 § TF som stadgar att om en myndighet bara har till uppgift att tekniskt bearbeta eller lagra en upptagning för automatiserad behandling för någon annan myndighets räkning, anses upptagningen inte vara en allmän handling hos den myndighet som bara har tekniska uppgifter i sammanhanget. Bestämmelsen sätter förvaringskriteriet i 2 kap. 4 § TF ur spel och har tillkommit mot bakgrund av att offentlighetsprincipen inte har ansetts kräva att allmänheten ska ha tillgång till en handling hos en myndighet som endast tar teknisk befattning med handlingen för annans räkning (prop. 1975/76:160 s. 87). Innebörden av paragrafen är att det väsentliga är om myndighetens enda syfte med handlingarna är teknisk bearbetning eller lagring. Om myndigheten av tekniska eller administrativa skäl har möjlighet att använda handlingarna på något annat sätt, är bestämmelsen inte tillämplig (jfr RÅ 1994 ref. 64).

9.3 Polismyndighetens tillgång till material från kamerabevakning genom samverkan

9.3.1 SOT-lösningen

Polismyndigheten har utvecklat en modell för samverkan med externa aktörer om kamerasystem och andra systemkomponenter som betecknas SOT (”säker oberoende transmission”). SOT-lösningen möjliggör för Polismyndigheten att ansluta sig till kamerasystem som ägs av externa aktörer, såväl enskilda som andra offentliga aktörer. När det gäller offentliga aktörer handlar det hittills i stor utsträckning om kommuner och regioner. Genom användning av SOT-lösningen kan Polismyndigheten direkt ta del av bildströmmar från en kamera som en samverkande part har satt upp, redan innan dessa bildströmmar har processats av den samverkande partens kamerabevakningssystem. SOT-lösningen kan i dagsläget enbart användas på strömmande bilder (videor).

SOT-lösningen är utformad i syfte att undvika att Polismyndighetens tillgång till material från andra aktörers kameror ska anses innefatta en situation där materialet lämnas ut från en personuppgiftsansvarig till en annan. Syftet med lösningens rättsliga och tekniska utformning är i stället att vardera samverkande part ska anses bedriva sin egen kamerabevakning, för vilken den parten är fullt ut ansvarig, men med hjälp av gemensam utrustning. På så sätt innebär SOT-lösningen bl.a. att man kan undvika att Polismyndigheten, i de situationer då myndigheten har ett intresse av och rättslig grund för att kamerabevaka samma plats som redan kamerabevakas av t.ex. en region, måste sätta upp sina egna fasta eller rörliga kameror bredvid regionens kameror. I stället kan båda aktörer bedriva kamerabevakning genom samma kamerasystem. Det är alltså inte fråga om att Polismyndigheten får tillgång till material från annans kamerabevakning och det behöver därmed inte göras någon sekretessbedömning av materialet.

Det har under arbetet med utredningen framkommit att Polismyndigheten fäster stort praktiskt värde vid SOT-lösningen. SOT-lösningen framstår som en effektiv och ändamålsenlig metod för att öka polisens tillgång till relevant bevakningsmaterial.

Beskrivning av SOT-lösningen

Samverkan inom ramen för SOT-lösningen kan ske med en annan offentlig aktör t.ex. en region. Regionen prioriterar platser för kamerabevakning utifrån sina egna behov och de rättsliga förutsättningar som gäller för regionen, bl.a. enligt kamerabevakningslagen. De prioriterade platserna kommer sedan undersökas av Polismyndigheten med avseende på problembild på platsen och eventuella kamerors placering. Polismyndigheten gör därefter en bedömning om de rättsliga förutsättningarna för polisen att kamerabevaka platsen är uppfyllda. Slutligen fattar Polismyndigheten ett beslut enligt kamerabevakningslagen om att inleda kamerabevakning på platsen i fråga. Detta beslut innefattar en intresseavvägning enligt 14 a och 14 b §§ jämte 8 § kamerabevakningslagen samt en proportionalitetsbedömning. En del i denna bedömning är att överväga hur stort kamerans bevakningsområde ska vara och om det, för att bevakningen ska vara proportionerlig, krävs att bildströmmarna från kameran förses med maskeringar. Maskering innebär att en del av kamerans upptagningsområde tas bort. Maskeringen är ”inbränd” i materialet, det vill säga den påverkar vilken bild som överhuvudtaget tas upp och lagras. Maskeringen går inte att lyfta vid bearbetning i efterhand. Om den samverkande aktören har en rörlig kamera, vilket enligt uppgift från Polismyndigheten är ovanligt, kommer bedömningen av vilket upptagningsområde som är proportionerligt och vilka maskeringar som behövs, göras med utgångspunkt i hela det möjliga upptagningsområdet för kameran.

Om Polismyndigheten och den samverkande aktören har avvikande behov av kamerabevakning, det vill säga om Polismyndigheten vill bevaka en större yta än den samverkande aktören, behöver myndigheten sätta upp en kompletterande kamera på platsen. Målsättningen vid SOT-lösningen är att i så stor utsträckning som möjligt hitta platser där både Polismyndigheten och den samverkande aktören har ett intresse och rättsliga förutsättningar att kamerabevaka. Samverkan mellan Polismyndigheten och den andra offentliga aktören, i detta exempel regionen, är i alla delar frivillig.

Efter det att Polismyndigheten fattat beslut om kamerabevakning kommer ett nyttjanderättsavtal upprättas mellan Polismyndigheten

och regionen, som alltså äger kameran. I avtalet regleras bl.a. frågor om kabeldragning, strömförsörjning, tillgång till internet m.m. I linje med att varje aktör ansvarar för sin egen kamerabevakning kommer också varje aktör att ansvara för att skylta och informera om sin kamerabevakning enligt de krav som gäller i kamerabevakningslagen och den dataskyddsrättsliga regleringen.

Överföring av bildströmmarna från kameran till Polismyndighetens kameraplattform sker krypterat. Polismyndigheten kan därefter bara komma åt materialet i kameraplattformen. Enligt Polismyndighetens gällande rutin lagras material från SOT-samverkan i kameraplattformen under 62 dygn. Därefter raderas det automatiskt. Det är endast behöriga användare hos Polismyndigheten som kan logga in i kameraplattformen och på så vis komma åt det lagrade materialet. Inloggning i kameraplattformen sker via tjänstekort och kräver angivande av tjänsteåtgärd och ärende. Alla händelser och aktiviteter som sker i kameraplattformen loggas.

Frågan om vilka tjänstemän inom Polismyndigheten som får fatta beslut om kamerabevakning och som får ingå nyttjanderättsavtal med samverkande aktörer inom ramen för SOT-lösningen regleras i myndighetens arbetsordning. Myndigheten har också tagit fram riktlinjer för kamerabevakning som sker på allmän plats. Utöver detta finns beslutsstöd till de tjänstemän som arbetar med frågorna i form av bl.a. interna utbildningar och nationella beslutsmallar.

Den överföring av bildströmmar till Polismyndigheten som sker inom ramen för SOT-lösningen sker genom samma mjukvara och använder samma kryptering som används i Polismyndighetens VPN-routrar när myndigheten sätter upp egna kameror.

Personuppgiftsansvar vid Polismyndighetens användning av SOT-lösningen

Polismyndighetens avsikt när det gäller SOT-lösningen är att myndigheten ska vara personuppgiftsansvarig för varje moment av den personuppgiftsbehandling som sker, det vill säga för insamling av material genom kamerabevakning, för överföringen till Polismyndighetens egna system och för den lagring som sedan sker hos myndigheten.

Det får anses sakna betydelse för bedömningen av personuppgiftsansvaret att Polismyndighetens och den samverkande partens kamerabevakning sker via samma kamera. Det väsentliga är i vilken mån Polismyndigheten uppfyller kraven för att betraktas som personuppgiftsansvarig enligt dataskyddsdirektivet och brottsdatalagen. I 1 kap. 6 § nämnda lag definieras personuppgiftsansvarig som "den behöriga myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter".

När SOT-lösningen används på det sätt som beskrivits i avsnitt 9.3.1 är det Polismyndigheten som självständigt bestämmer ändamålen med och medlen för varje led av den personuppgiftsbehandling som sker hos Polismyndigheten.

Vad beträffar det första ledet i personuppgiftsbehandlingen, själva insamlingen, kan konstateras att Polismyndigheten självständigt förfogar över samtliga nyckelmoment i kamerabevakningen. Myndigheten beslutar att kamerabevakning ska ske på en viss plats, i vilket syfte det ska ske och varför. På samma sätt förfogar den samverkande parten självständigt över samtliga nyckelelement i anslutning till sin kamerabevakning. Ingendera parten har möjlighet att bestämma över den andra parten eller påverka dennes bedömningar. Att den andra offentliga aktören måste vilja samverka för att SOT-lösningen ska vara möjlig att genomföra framstår som en fråga om rent praktiska förutsättningar och inte ett moment som i och för sig gör Polismyndighetens beslut mindre självständigt.

Det har framkommit att det i en tidigare version av mallarna till de nyttjanderättsavtal som Polismyndigheten använder sig av inom ramen för SOT-lösningen föreskrevs att fastighetsägaren, det vill säga den samverkande aktören, inte fick ändra kamerans upptagningsområde utan Polismyndighetens godkännande. Vidare föreskrevs att om en fastighetsägare avsåg att montera ned en kamera eller övrig utrustning skulle det föregås av en dialog med Polismyndigheten. Mot bakgrund av detta ansåg Integritetsskyddsmyndigheten – i en skrivelse daterad den 21 december 2023 som svar på en förfrågan från Polismyndigheten beträffande dataskyddsrättsliga aspekter på SOT-lösningen – att det kunde ifrågasättas om den externa aktören som Polismyndigheten samverkar med inom ramen för SOT-lösningen var att betrakta som

helt självständig i sin personuppgiftsbehandling, såtillvida att aktören inte själv kunde bestämma över medlen för sin personuppgiftsbehandling (Integritetsskyddsmyndigheten, Svar på förfrågan avseende Polismyndighetens kamerabevakning med SOT-lösning, dnr IMY-2023-8726).

Integritetsskyddsmyndigheten ifrågasatte vidare om det var rättsligt möjligt att ha ett gemensamt personuppgiftsansvar mellan Polismyndigheten och en samverkande aktör i form av t.ex. en region, mot bakgrund av att Polismyndighetens personuppgiftsbehandling (inom ramen för den brottsbekämpande verksamheten) regleras av brottsdatalagen och dataskyddsdirektivet, medan regionens personuppgiftsbehandling regleras av dataskyddsförordningen. Dessa regelverk motsvarar inte varandra helt när det gäller förutsättningar för gemensamt personuppgiftsansvar. Exempelvis innehåller dataskyddsförordningen särskilda regler om att det ska finnas ett inbördes arrangemang mellan gemensamt person-uppgiftsansvariga som ska fördela deras skyldigheter enligt förordningen, och att den registrerade ska kunna vända sig till var och en av de personuppgiftsansvariga för att utöva sina rättigheter (artikel 26). Integritetsskyddsmyndigheten konstaterade att det var oklart hur dessa skyldigheter skulle kunna uppfyllas av en personuppgiftsansvarig vars behandling inte omfattas av dataskyddsförordningen.

Polismyndigheten har upplyst om att myndigheten, med anledning av Integritetskyddsmyndighetens skrivelse, har justerat sina mallar för de nyttjanderättsavtal som används inom ramen för SOT-lösningen. I avtalen finns nu endast en skyldighet för en fastighetsägare att meddela Polismyndigheten om eventuella förändringar av kamerans upptagningsområde, i syfte att Polismyndigheten ska kunna säkerställa att myndighetens kamerabevakning vid var tid är lagenlig. Med anledning av de reviderade versionerna av nyttjanderättsavtalen får frågetecknen gällande om Polismyndigheten och de externa samverkande aktörerna är var för sig självständigt personuppgiftsansvariga anses ha undanröjts. Att det föreligger en avtalsenlig förpliktelse att meddela när vissa åtgärder vidtas kan inte i sig anses minska avtalspartens rätt eller möjlighet att självständigt råda över saken på grundval av sina egna bedömningar. Polismyndigheten får därför anses vara ensam personuppgiftsansvarig för den behandling av personuppgifter som

sker genom myndighetens kamerabevakning inom ramen för SOT-lösningen.

Vad sedan beträffar frågan om överföringen av det material och de personuppgifter som samlas in genom kamerabevakning får Polismyndigheten även i det ledet anses vara självständigt personuppgiftsansvarig. Polismyndigheten bestämmer som sagt självständigt över vilka ändamål och med vilka medel som kamerabevakningen bedrivs och har även teknisk kontroll över på vilket sätt överföringen sker till myndighetens kameraplattform. Den samverkande parten kan inte heller ta del av eller bearbeta det videomaterial som förs över till Polismyndighetens kameraplattform.

Vad slutligen beträffar frågan om lagring av personuppgifter, som är det sista ledet i personuppgiftsbehandlingen, framgår det av Polismyndighetens redogörelse för SOT-lösningen att lagring av kamerabevakningsmaterialet sker på samma sätt i kameraplattformen oavsett om materialet genereras av en kamera som ägs av en samverkande part, eller om materialet genereras av en kamera som ägs av Polismyndigheten. Den samverkande parten har ingen möjlighet att bearbeta eller tillgå det material som Polismyndigheten lagrar. Polismyndigheten får anses ensamt personuppgiftsansvarig även för lagringen av uppgifterna.

Sammantaget får därmed den bedömningen göras att Polismyndigheten är ensam personuppgiftsansvarig för hela processen. I samtliga led har båda parter sin egen rättsliga grund för behandlingen och ingen av de samverkande parterna kan sägas bedriva kamerabevakning för den andres räkning. Därtill bör rimligen materialet utgöra allmänna handlingar hos båda myndigheterna eftersom det inte är fråga om vare sig en direktåtkomst för Polismyndigheten eller ett elektroniskt utlämnande till myndigheten på annat sätt. Detta innebär att vardera myndigheten, vid en begäran om att få ta del av materialet från kamerorna, får göra en bedömning av om materialet är sådant att det kan lämnas ut.

9.4 Olika sätt för Polismyndigheten att ta del av material från andra offentliga aktörers bevakningskameror

Polismyndigheten kan alltid begära ut material från andra aktörers bevakningskameror med stöd av 6 kap. 5 § OSL. Vid en sådan begäran måste den utlämnande myndigheten göra en sekretessbedömning innan materialet lämnas ut. I de fall det finns en uppgiftsskyldighet reglerad i lag[18] kan materialet lämnas ut med stöd av denna och en sekretessbedömning behöver då inte ske. I de fall det handlar om material som innehåller personuppgifter måste utlämnandet även vara förenlig med den dataskyddsrättsliga regleringen.

Som framgått ovan innebär SOT-lösningen inte att Polismyndigheten begär och tar del av material från en annan aktörs kamerabevakning. Det är en effektiv lösning då Polismyndigheten får del av material från kamerabevakning direkt utan att det föregås av en sekretessprövning. SOT-lösningen kan dock bara användas på platser där Polismyndigheten enligt kamerabevakningslagen själv kan bedriva kamerabevakning och användningen av lösningen är därför begränsad. En ytterligare begränsning är att SOT-lösningen enbart kan användas för strömmande bilder. Det innebär att en SOT-lösning inte är en möjlig teknik för informationsdelning avseende material exempelvis från flera av de kameror som Trafikverket har uppsatta. Kameror som används för att ta ut trängselskatt och infrastrukturavgift samt trafiksäkerhetskameror genererar enbart stillbilder. Även Tullverkets kameror genererar stillbilder. I dagsläget finns inga planer på att utöka funktionaliteten i trafiksäkerhetskamerorna till strömmande bilder, bl.a. på grund av dataöverföringskapacitet.

Den tekniska lösning som i dagsläget finns tillgänglig för Polismyndigheten att löpande ta del av stillbilder från Trafikverkets kameror är samma lösning som används när material från kameror som är uppsatta för att kunna ta ut trängselskatt eller infrastrukturavgift lämnas ut till Transportstyrelsen. Detta innebär att Polismyndigheten skulle få 5 000 passagebilder per gång vid flera tillfällen per dygn eller var femte minut. Ett sådant informationsutbyte skulle i dagsläget innebära en stor personell insats av Polismyndigheten,

[18] Se exempelvis 5 kap. 3 a § vägtrafikdataförordningen (2019:382).

eftersom det krävs en manuell granskning och bearbetning av bilderna då det saknas en programvara som kan göra detta. Bilderna skulle inte heller bli tillgängliga för Polismyndigheten direkt, eftersom det skulle ta lång tid att gå igenom dem när de inkommer till myndigheten. Som utgångspunkt innehåller passagebilderna endast ett registreringsnummer. Vem som kör bilen eller vilket märke det är på bilen framgår vanligtvis inte. Det kan ifrågasättas om tillgång till bilderna tillgodoser det behov som Polismyndigheten har framfört.

Polismyndigheten har uttryckt att myndigheten, för att kunna utföra sitt uppdrag på ett effektivt sätt, skulle vara behjälpt av att kunna ta del av material från andra aktörers kamerabevakning via en fjärråtkomst, både inspelat och i realtid. Önskemålet avser framför allt material från Trafikverkets kameror vid järnvägsplattformar och i tunnlar samt sådana som används för att se vägars ytskikt. Dessa kameror genererar strömmande bilder och ger en aktuell översiktsbild över platsen där kameran finns. Alla kameror i tunnlar och kameror som används för att se vägars ytskikt spelar dock inte in material. Materialet från dessa kameror innehåller vanligen inga personuppgifter eller detaljerade uppgifter om fordon, även om de i någon utsträckning kan ge en bild av vilka fordon som rör sig på de aktuella platserna. Material från kamerorna vid järnvägsplattformar är mer detaljrika och kan användas för att identifiera personer.

Trafikverket har upplyst om att det i dagsläget saknas en teknisk möjlighet för Polismyndigheten att få tillgång till strömmande bilder från Trafikverkets kameror via en SOT-lösning. Vid operativt läge har Polismyndigheten möjlighet att ta del av strömmande bilder från Trafikverkets kameror på plats hos Trafikverket. Detta sker genom att poliser kommer till Trafikverkets trafikledningscentral där operatörerna har tillgång till material, både i realtid och inspelat. I dessa fall gör operatören eller en arbetsledande funktion en sekretessbedömning innan poliserna får ta del av materialet. Arbetssättet kommer ofta i konflikt med det uppdrag som Trafikverket har och leder till, enligt verket, en stor påfrestning på den operativa verksamheten, eftersom hanteringen tar resurser i anspråk.

I dagsläget finns en teknisk lösning tillgänglig som möjliggör för Polismyndigheten att ta del av strömmande bilder från Trafikverkets kameror vid järnvägsplattformar. Detta sker genom en s.k. Citrix-

lösning. Lösningen innebär att information delas via ett virtuellt skrivbord som ger Polismyndigheten tillgång till Trafikverkets kameraplattform för kameror uppsatta för att bevaka järnvägsanläggningar. Denna lösning ger Polismyndigheten tillgång till Trafikverkets kameror på ett säkert och kontrollerat sätt. En förutsättning är att uppgifterna inte bedöms omfattas av sekretess. Det går att reglera tillgången till materialet genom att begränsa Polismyndighetens behörighet till kameror och tider som är relevanta i ett aktuellt ärende. Det går också att vid delning av materialet välja att bara dela material från en specifik plats, exempelvis en viss järnvägsstation. Lösningen tillåter inte att Polismyndigheten sparar ner eller exporterar videoströmmar. Polismyndigheten kan dock själv söka i materialet, både strömmande bilder i realtid och inspelat material, och förbereda vad som ska delas. Denna lösning uppfyller enligt Polismyndigheten inte myndighetens behov, främst eftersom det virtuella skrivbordet inte kan sammanfogas med myndighetens eget kamerasystem och därmed inte ge den helhetsbild av alla tillgängliga kameror som behövs utifrån ett verksamhetsperspektiv. För att möjliggöra åtkomst till Trafikverkets kameror behöver lösningen byggas ut och anpassas. Tidsmässigt skulle lösningen kunna etableras snabbare än om en helt ny teknisk lösning för att föra över videoströmmar till Polismyndigheten skulle tas fram.

10 Ansiktsigenkänning

10.1 Inledning

Ansiktsigenkänning är en digital teknik för att automatiskt identifiera en person eller verifiera en viss persons identitet utifrån en digital bild. Det görs vanligen genom att utvalda ansiktsdrag från en bild jämförs med bilder på ansikten som sammanställts i en databas. Användandet av teknik för ansiktsigenkänning innebär en behandling av biometriska uppgifter. Biometriska uppgifter är en typ av personuppgifter som anses vara känsliga. Behandlingen av sådana uppgifter är därmed särskilt reglerade i brottsdatalagen och polisens brottsdatalag. I avsnittet beskrivs begreppet biometriska uppgifter, hur sådana uppgifter får behandlas och hur Polismyndigheten använder sig av ansiktsigenkänning i sin verksamhet i dagsläget. Det redogörs även i korthet för EU:s förordning om artificiell intelligens (AI)[19].

Biometriutredningen har i betänkandet *Biometri – för en effektivare brottsbekämpning* (SOU 2023:32) lämnat förslag på utökade möjligheter att använda biometriska data i brottsbekämpningen. Förslagen har ännu inte lett till lagstiftning.

[19] Europaparlamentets ståndpunkt fastställd vid första behandlingen den 13 mars 2024 inför antagandet av Europaparlamentets och rådets förordning (EU) 2024/… om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (rättsakt om artificiell intelligens).

10.2 Biometriska uppgifter

10.2.1 Begreppet biometriska uppgifter

Vad som utgör biometriska uppgifter definieras i 1 kap. 6 § brottsdatalagen. Av bestämmelsen framgår att begreppet avser uppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen. Samma definition finns även i 1 kap. 5 § säkerhetspolisens datalag. Definitionen utgår från den som finns i artikel 3.13 dataskyddsdirektivet. För att det ska vara fråga om biometriska uppgifter krävs att uppgifterna bearbetats tekniskt genom en särskild metod som syftar till identifiering. Vanliga fotografier och filmer omfattas alltså inte av definitionen (prop. 2017/18:232 s. 86).

Exempel på individuella kännetecken som kan användas för biometrisk analys är t.ex. dna, mönster av fingeravtryck, ansiktsgeometri, ögats iris, röst, händer, blodkärl och gångstil. Biometriska uppgifter är information som kan tas fram ur ett sådant underlag. Uppgifterna kan användas för att skapa en referensmall eller för att jämföra med tidigare lagrade referensmallar i syfte att kontrollera en persons identitet. Analys av spår från t.ex. en brottsplats utgör biometriska uppgifter även om det, när analysen genomförs, inte går att härleda spåren till en identifierad person. Detta eftersom det med hjälp av en sådan analys går att identifiera den person som har avsatt spåren. Teknisk bearbetning av foto och videomaterial som inte sker i syfte att åstadkomma unik identifiering faller dock utanför definitionen. Det innebär att bearbetning av bilder av personer för att förbättra bildkvaliteten, förstärka detaljer och liknande inte omfattas av definitionen, till skillnad från bilder som bearbetas i exempelvis ett ansiktsigenkänningsprogram i syfte att identifiera personer (jfr prop. 2017/18:232 s. 435).

10.2.2 Behandling av biometriska uppgifter

Biometriska uppgifter utgör s.k. känsliga personuppgifter. Dessa är särskilt skyddsvärda och får enligt 2 kap. 12 § brottsdatalagen endast behandlas om det är särskilt föreskrivet och absolut nödvändigt för ändamålet med behandlingen. Att behandling av biometriska upp-

gifter endast får ske om det är absolut nödvändigt för ändamålet med behandlingen framgår även av 2 kap. 4 § och 6 kap. 4 § polisens brottsdatalag. Att behandlingen måste vara absolut nödvändig innebär att behovet av att behandla sådana uppgifter måste prövas särskilt noga i det enskilda fallet (prop. 2017/18:232 s. 447 f. och prop. 2017/18:269 s. 296).

Bestämmelserna i brottsdatalagen och polisens brottsdatalag har sitt ursprung i artikel 10 i dataskyddsdirektivet. Artikeln föreskriver att behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, samt behandling av genetiska uppgifter, biometriska uppgifter för att unikt identifiera en fysisk person eller uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara tillåten endast om det är absolut nödvändigt och under förutsättning att det finns lämpliga skyddsåtgärder för den registrerades rättigheter och friheter och endast om behandlingen är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan fysisk person eller om behandlingen rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade. Precis som vid all personuppgiftsbehandling måste behandling av biometriska uppgifter för att entydigt identifiera en fysisk person ske i överensstämmelse med de grundläggande principerna för behandling av personuppgifter som framgår av artikel 4 dataskyddsdirektivet. För att behandlingen inte ska komma i konflikt med grundläggande principer krävs att ändamålet med behandlingen inte kan uppnås på ett mindre integritetskänsligt sätt.

När personuppgiftsbehandling sker genom ansiktsigenkänning ska vanligen en konsekvensbedömning göras. Beroende på resultatet av bedömningen kan det även bli aktuellt att genomföra ett förhandssamråd med tillsynsmyndigheten (se 3 kap. 7 § brottsdatalagen).

EU-domstolen har funnit att nationell lagstiftning, vilken föreskriver en systematisk insamling av biometriska uppgifter för varje person som misstänks för ett uppsåtligt brott som omfattas av allmänt åtal, i princip strider mot kravet att behandling får ske endast om det är absolut nödvändigt i artikel 10 dataskyddsdirektivet. En sådan lagstiftning kan nämligen leda till en insamling av biometriska

uppgifter, utan åtskillnad och generellt, om de flesta misstänkta personer, eftersom begreppet ”uppsåtligt brott som omfattas av allmänt åtal” är av särskilt allmän karaktär och kan tillämpas på ett stort antal brott, oberoende av deras art och allvar. Enligt en sådan lagstiftning begränsas visserligen tillämpningsområdet för insamlingen av biometriska och genetiska uppgifter till personer som är föremål för en förundersökning under det straffrättsliga förfarandet, det vill säga personer avseende vilka det finns tungt vägande skäl att anta att de har begått ett brott i den mening som avses i artikel 6 a dataskyddsdirektivet. Enbart den omständigheten att en person misstänks för ett uppsåtligt brott som omfattas av allmänt åtal kan emellertid inte i sig anses utgöra en omständighet som gör det möjligt att anta att insamlingen av vederbörandes biometriska och genetiska uppgifter är absolut nödvändig med hänsyn till ändamålen för denna insamling och de kränkningar av de grundläggande rättigheterna, i synnerhet rätten till respekt för privatlivet och skyddet för personuppgifter enligt artiklarna 7 och 8 i stadgan, som insamlingen ger upphov till (*EU-domstolens dom av den 26 januari 2023 V.S. mot Ministerstvo na vatreshnite raboti m.fl., C 205/21, EU:C:2023:49, p. 128-130*).

Europeiska dataskyddsstyrelsen (EDPB), som är ett oberoende europeiskt organ som ser till att dataskyddsförordningen och dataskyddsdirektivet tillämpas enhetligt, har antagit riktlinjer om brottsbekämpande myndigheters användning av ansiktsigenkänning (05/2022). Av dessa framgår att användning av ansiktsigenkänning måste följa gällande regler och framför allt de krav på nödvändighet och proportionalitet som EU-stadgan om de grundläggande rättigheter ställer upp. Av riktlinjerna framgår även att EDPB anser att biometrisk fjärridentifiering på allmänt tillgängliga platser utgör en stor risk för ingrepp i privatlivet och inte är hemmahörande i ett demokratiskt samhälle eftersom det ger möjlighet till massövervakning.

10.3 Polismyndighetens användning av ansiktsigenkänning

Den som begår ett brott lämnar i många fall spår efter sig. Gärningspersonen kan bl.a. ha fångats på bild av en bevaknings-

kamera eller av någon som har filmat eller tagit bilder med en mobiltelefon. I de fall det inte finns en misstänkt gärningsperson är det nödvändigt att kunna jämföra spår från brottsutredningen med registrerade dna-profiler, fingeravtryck och andra biometriska uppgifter för att öka möjligheterna att klara upp brottet. När Polismyndigheten söker i register med hjälp av bl.a. ansiktsbilder behandlar myndigheten biometriska uppgifter. (Jfr SOU 2023:32 s. 211.)

Möjligheten att identifiera personer med hjälp av biometri har utvecklats mycket snabbt på senare tid. Det gäller inte minst teknik för avancerad ansiktsigenkänning. När det gäller fotografier finns helt andra möjligheter än tidigare att med hjälp av t.ex. program för ansiktsigenkänning identifiera okända gärningspersoner. (Se a. SOU s. 21 och 260.)

Det förekommer över lag en ökad användning av ansiktsbilder i samhället. Det hänger i hög utsträckning samman med den tekniska utvecklingen och att fotografier på papper har ersatts av digitala motsvarigheter. Numera är det normalt sett också digitala versioner av fotografier av misstänkta som sparas i Polismyndighetens signalementsregister. Härigenom har det skapats möjligheter att upprätta effektiva och sökbara register och att använda sig av bilder för ansiktsigenkänning. (Se a. SOU s. 221.) Behörigheten för Polismyndigheten att föra signalementsregister, vilket innehåll registret får ha, längsta tid för behandling av uppgifterna och direktåtkomst till registret regleras i 5 kap. 11–17 §§ polisens brottsdatalag. År 2021 innehöll signalementsregistret 67 156 digitala ansiktsbilder. Utöver ansiktsbilder innehåller registret också bl.a. helkroppsbilder och bilder på särskilda kännetecken som tatueringar och ärr (Se a. SOU s. 188.)

Möjligheterna för Polismyndigheten att behandla personuppgifter för forensiska ändamål regleras i 6 kap. polisens brottsdatalag. Av 1–3 §§ framgår för vilka ändamål personuppgifter får behandlas. I 5 § föreskrivs att sökförbudet i 2 kap. 14 § brottsdatalagen inte hindrar sökningar i personuppgifter som behandlas i registren över dna-profiler eller fingeravtrycks- och signalementsregistren, i syfte att få fram ett urval av personer grundat på uppgifter som rör hälsa eller biometriska eller genetiska uppgifter.

I dag används ansiktsigenkänning som ett verktyg inom Polismyndigheten genom registersökning av ansiktsbild och automatisk

bildanalys. En detaljerad beskrivning av metoderna görs i SOU 2023:32 (s. 221 ff.) och redogörs för i korthet nedan.

Ansiktsigenkänning för automatiska jämförelser i signalementsregistret sker sedan år 2021 inom ramen för den forensiska undersökningen av Nationellt forensiskt centrum (NFC). Ansiktsigenkänning för automatiska jämförelser i signalementsregistret sker genom att en bild på en okänd person söks mot registrerade ansiktsbilder i signalementsregistret i syfte att få fram ett uppslag på vem personen är eller kan vara. NFC använder en mjukvara för ansiktsigenkänning för att söka spårbilden mot ansiktsbilderna i signalementsregistret. Registret innehåller sökfunktionalitet för de registrerade ansiktsbilderna vilket möjliggör ansiktsigenkänning. Mjukvaran returnerar en söklista med de bästa matchningarna. Söklistan analyseras därefter manuellt av en handläggare vid NFC, som gör en sammantagen bedömning av om en potentiell kandidat förekommer i listan eller inte. Datainspektionen (numera Integritetsskyddsmyndigheten) har bedömt att det inte finns något hinder för polisen att använda en programvara för ansiktsigenkänning mot signalementsregistret för att identifiera gärningspersoner inom den forensiska verksamheten (Datainspektionen, Förhandssamråd om Polismyndighetens planerade användning av programvara för ansiktsigenkänning mot signalementsregistret, 2019-10-23, dnr DI-2019-10508).

Metoden automatisk bildanalys används av Polismyndigheten inom förundersökningar sedan år 2021. Metoden innebär att stora mängder bilder och videomaterial insamlade från exempelvis kamerabevakning på allmän plats eller i kollektivtrafiken behandlas med automatiska bildanalysalgoritmer. Syftet med metoden är inte att identifiera någon genom en sökning mot ett register med kända personer, och inte heller att lagra informationen i ett register, utan endast att temporärt behandla uppgifterna för att påskynda processen vid analysarbetet.

10.3.1 Särskilt om ”krunchning”

”Krunchning” används ibland som term för en teknik som innebär att bild- och filmmaterial behandlas med AI-baserade bildanalysalgoritmer som extraherar viss information om innehållet i

materialet. Tekniken möjliggör filtrering och sortering av ett material och dess innehåll. De algoritmer som används bestämmer närmare vilken information som extraheras.

Krunchning kan bl.a. ske av bild- och filmmaterial, i syfte att materialet därefter ska kunna användas för ansiktsigenkänningsändamål. Sådan krunchning går till på i huvudsak följande sätt. En första AI-algoritm hittar ansikten i bild- eller filmmaterialet och extraherar dessa ansiktsbilder från materialet. En andra AI-algoritm tar därefter vid och extraherar en digital representation av ansiktena ur de ansiktsbilder som den första algoritmen har identifierat och extraherat. En digital representation som skapas på detta sätt kallas även för en template eller en feature-vektor. Den digitala representationen utgörs av hundratals numeriska värden som på ett abstrakt sätt beskriver ansiktets utseende. Det rör sig exempelvis om angivelser om avstånd mellan olika punkter i ansiktet och dessa punkters läge i förhållande till varandra. Syftet är att den digitala representationen ska vara så unik som möjligt för varje avbildad person. Informationen som på detta sätt extraheras vid krunchning lagras i en temporär databas (indexeringsdatabas) vid sidan av det insamlade kameramaterialet. Databasen sparas endast så länge som kameramaterialet sparas. Inga identiteter är kända eller kopplade till de ansiktsbilder som samlas in i databasen.

Det görs inga jämförelser mellan olika digitala representationer och i detta skede beräknas inte heller några likhetsmått mellan olika digitala representationer. Först i steget efter att krunchningen har gjorts vidtar en eventuell ansiktsigenkänning, det vill säga en jämförelse och ett försök till matchning mellan den lagrade digitala representationen och en referensbild av en människa, vars identitet kan vara känd eller okänd.

Krunchning innebär alltså att ett material bearbetas för att, vid en senare tidpunkt, kunna jämföras med andra bilder. Det kan t.ex. röra sig om jämförelsebilder hämtade från ett register (som misstankeregistret) eller från en bevakningskamera. Tekniken används i dagsläget av Polismyndigheten som ett förberedande steg för ansiktsigenkänning och utförs i anslutning till att myndigheten ska utföra ansiktsigenkänning på ett visst material, när de rättsliga förutsättningarna och polisiära behoven för detta föreligger.

10.4 EU:s AI-förordning

Den 13 mars 2024 antogs texten till den kommande AI-förordningen[20]. Av artikel 1.1 framgår att syftet med förordningen är att förbättra den inre marknadens funktion och främja användningen av människocentrerad och tillförlitlig AI, samtidigt som en hög skyddsnivå säkerställs för hälsa, säkerhet och grundläggande rättigheter som fastställs i stadgan om de grundläggande rättigheterna, inbegripet demokrati, rättsstatsprincipen och miljöskydd, mot de skadliga effekterna av AI-system i unionen, och att stödja innovation. Förordningens bestämmelser påverkar inte tillämpningen av befintlig unionslagstiftning om behandling av personuppgifter (se skäl 10).

Förordningen bygger på en riskbaserad metod, där olika AI-system regleras på olika sätt beroende på vilken risk systemet anses utgöra. Med risk avses kombinationen av sannolikheten för skada och denna skadas allvarlighetsgrad (artikel 3.2). Ett exempel på högrisksystem är alla system för biometrisk fjärridentifiering (se skäl 54). Sådana system omfattas därför av strikta krav i förordningen.

Med begreppet biometriska uppgifter avses i förordningen personuppgifter som erhållits genom särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken, såsom ansiktsbilder eller fingeravtrycksuppgifter (artikel 3.34). Biometrisk identifiering definieras som automatiserad igenkänning av fysiska, fysiologiska, beteendemässiga eller psykologiska mänskliga särdrag för att fastställa en fysisk persons identitet genom jämförelse av personens biometriska uppgifter med biometriska uppgifter om enskilda personer som lagrats i en databas (artikel 3.35).

Förordningens definition av system för biometrisk fjärr-identifiering är ett AI-system vars syfte är att identifiera fysiska personer utan deras aktiva medverkan, vanligtvis på distans, genom jämförelse av en persons biometriska uppgifter med de biometriska uppgifterna i en referensdatabas (artikel 3.41). Av skäl 17 framgår bl.a. att begreppet bör definieras utifrån funktion som ett AI-system

[20] Europaparlamentets ståndpunkt fastställd vid första behandlingen den 13 mars 2024 inför antagandet av Europaparlamentets och rådets förordning (EU) 2024/… om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (rättsakt om artificiell intelligens).

avsett för identifiering av fysiska personer utan deras aktiva medverkan, vanligtvis på distans, genom jämförelse mellan en persons biometriska uppgifter och biometriska uppgifter i en referensdatabas, oavsett den specifika teknik, process eller typ av biometriska uppgifter som används. Sådana system för biometrisk fjärridentifiering används vanligtvis för att samtidigt uppfatta flera personer eller deras beteende för att avsevärt underlätta identifieringen av fysiska personer utan deras aktiva medverkan. Definitionen utesluter AI-system som är avsedda att användas för biometrisk verifiering, vilket inbegriper autentisering, vars enda syfte är att bekräfta att en specifik fysisk person är den person som denne utger sig för att vara, och system som används för att bekräfta identiteten för en fysisk person med det enda syftet att få åtkomst till en tjänst, låsa upp en enhet eller ha säker tillgång till lokaler. Undantaget motiveras av att sådana system sannolikt har mindre inverkan på fysiska personers grundläggande rättigheter än de system för biometrisk fjärridentifiering som kan användas för behandling av biometriska uppgifter om ett stort antal personer utan deras aktiva medverkan.

Användning av biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpande ändamål är som utgångspunkt inte tillåten enligt förordningen (artikel 5.1 h). Med realtid avses att insamling av biometriska uppgifter, jämförelse och identifiering sker utan betydande dröjsmål och omfattar inte bara omedelbar identifiering utan även begränsade korta fördröjningar för att undvika kringgående (artikel 3.42). Med system för biometrisk fjärridentifiering i efterhand avses ett annat system för biometrisk fjärridentifiering än ett system för biometrisk fjärridentifiering i realtid (artikel 3.43). Av skäl 17 framgår att när det gäller system i realtid sker insamlingen av biometriska uppgifter, jämförelsen och identifieringen omedelbart, näst intill omedelbart eller under alla omständigheter utan betydande dröjsmål. I detta avseende bör det inte finnas något utrymme för att kringgå AI-förordningens regler om användning i realtid av de berörda AI-systemen genom att medge mindre fördröjningar. Realtidssystem involverar direktupptagningar eller näst intill direktupptagningar av material, såsom videoupptagningar, genererade med kamera eller annan utrustning med liknande funktion.

Med allmänt tillgänglig plats avses varje offentligt eller privat ägd fysisk plats som är tillgänglig för ett obestämt antal fysiska personer, utan hänsyn till om vissa villkor eller omständigheter för tillträde kan gälla, och oberoende av eventuella kapacitetsbegränsningar (artikel 3.44). Med brottsbekämpande myndighet avses en offentlig myndighet som har behörighet att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inbegripet att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, eller ett annat organ eller en annan enhet som genom medlemsstaternas nationella rätt har anförtrotts myndighetsutövning för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inbegripet att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten (artikel 3.45).

Av artikel 5 framgår emellertid att medlemsstaterna får föreskriva att biometrisk fjärridentifiering i realtid för brottsbekämpande ändamål får användas, under vissa förutsättningar, endast när det är absolut nödvändigt i vissa begränsade situationer bl.a. när det är nödvändigt för att söka efter ett försvunnet barn, för att förhindra ett specifikt och överhängande terroristhot eller för att upptäcka, lokalisera, identifiera eller lagföra en förövare eller misstänkt för ett allvarligt brott. För att få använda ett sådant system krävs tillstånd från ett rättsligt eller annat oberoende organ. Det krävs även lämpliga begränsningar i tid, geografisk räckvidd och de databaser som har sökts. Artikeln reglerar också hur utdata från systemet för biometrisk fjärridentifiering i realtid får användas.

11 Överväganden

11.1 Inledning

Polismyndigheten har till uppgift att förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten, övervaka den allmänna ordningen och säkerheten och ingripa när störningar har inträffat, liksom att utreda och beivra brott som hör under allmänt åtal (2 § polislagen). Till Säkerhetspolisens uppdrag hör bl.a. att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott samt att utreda och beivra sådana brott. När Säkerhetspolisen leder polisverksamhet ska det som i lag eller annan författning föreskrivs om Polismyndigheten i tillämpliga delar gälla Säkerhetspolisen (3 § polislagen).

Polismyndighetens och Säkerhetspolisens lagstadgade uppgifter svarar mot ett mycket angeläget allmänt intresse. För att kunna genomföra sitt uppdrag har båda myndigheterna ett grundläggande behov av att i olika sammanhang kunna samla in, analysera, bearbeta och lagra uppgifter av olika slag, däribland personuppgifter. Detta kan bl.a. ske genom kamerabevakning. När kamerabevakning bedrivs på ett sätt som innebär att personuppgifter samlas in utgör den ett ingrepp i den personliga integriteten. Sådan kamerabevakning måste alltid vara proportionerlig sett till syftet med bevakningen. Det som kan anses vara proportionerligt varierar över tid, plats och övriga omständigheter. Kamerabevakning som är proportionerlig under viss tid och på viss plats kan således vara oproportionerlig under annan tid eller på annan plats. Ett större ingrepp i den personliga integriteten kan i vissa fall vara befogat, särskilt om det behövs för att ge brottsbekämpande myndigheter ett effektivt sätt att förebygga, förhindra, upptäcka, utreda eller lagföra brott. Inte minst gäller detta grov brottslighet. I sammanhanget bör

hållas i minnet att av bl.a. Europakonventionen följer att staten har en skyldighet att skydda enskilda mot intrång i deras rättigheter från andra enskilda (jfr prop. 2022/23:106 s. 13 och prop. 2022/23:126 s. 64).

Kamerabevakning kan utgöra ett medel för att öka tryggheten i samhället och minska risken för enskilda att utsättas för brott. Samhällets krav på att brott bekämpas på ett effektivt sätt och de verktyg som ges de brottsbekämpande myndigheterna för att utföra sitt uppdrag måste alltid balanseras på ett rimligt sätt mot den enskildes rätt till skydd mot intrång i den personliga integriteten. Beroende på hur samhällssituationen ser ut kan denna balansgång ge olika resultat. Något som bl.a. måste beaktas är den tekniska utvecklingen. Teknikutvecklingen kan utgöra argument både för och emot att utöka brottsbekämpande myndigheters legala möjligheter att samla in och använda personuppgifter.

Å ena sedan innebär teknikutvecklingen nya möjligheter för effektiviserad brottsbekämpning, bl.a. genom att information kan samlas in, bearbetas och analyseras på ett sätt som tidigare inte varit möjligt. Exempelvis kan automatiserade analyser och jämförelser ersätta tidskrävande manuella analyser som i praktiken ibland kanske inte ens är möjliga att göra. Automatiserad analys med viss mänsklig inblandning kan innebära att kontroller, bevakning, ingripanden och andra åtgärder kan göras mer träffsäkra, vilket i sin tur innebär att risken för intrång i den enskildes integritet minskar till skillnad från om analysen görs uteslutande av människor. Regeringen har tidigare betonat att en väl utnyttjad informationsteknik är av stor betydelse för polisens möjligheter att bedriva sin verksamhet på ett effektivt och rättssäkert sätt (prop. 2009/10:85 s. 59). Regeringen har också uttryckt att möjligheterna att använda kamerabevakning som ett naturligt hjälpmedel i det brottsbekämpande arbetet bör öka (prop. 2017/18:231 s. 65).

Å andra sidan kan teknikutvecklingen ge särskild anledning till noggranna överväganden om integritetsskydd. Personuppgifter som samlas in genom kamerabevakning bl.a. i förening med teknik för automatisk igenkänning och analys kan innebära särskilda risker för intrång i enskildas integritet. Detta till följd av bl.a. de möjligheter som tekniken innebär att bevaka och kartlägga ett mycket stort antal människor. Det är därför viktigt att användningen av sådan teknik är reglerad i lag så att den kan ske på ett ordnat, begränsat och

förutsägbart sätt. På det sättet kan respekten för den enskildes integritet upprätthållas samtidigt som användning av kamerateknik i bevakningssyften kan ske för berättigade ändamål i den omfattning som krävs. All lagstiftning som innebär att olika aktörer får behandla personuppgifter måste också överensstämma med den dataskyddsrättsliga regleringen, som ger ett robust och väl avvägt skydd för det intrång som behandlingen av personuppgifter i brottsbekämpande myndigheters verksamhet ibland innebär.

Information är viktigt i Polismyndigheten och Säkerhetspolisens arbete. För att brottsbekämpning ska kunna ske effektivt är det viktigt att Polismyndigheten och Säkerhetspolisen ges möjlighet att ta del av information från andra aktörer och sådan som finns inom den egna verksamheten. När rätt personer får del av rätt information kan flera effektivitetsvinster uppnås. Informationsdelningen måste dock alltid ske på ett sätt som inte innebär otillbörliga intrång i den personliga integriteten.

Något som måste beaktas i balansgången mellan en effektiv brottsbekämpning och skyddet för den personliga integriteten är hur den aktuella brottsligheten ser ut i samhället. Organiserad brottslighet och terroristbrottslighet utgör allvarliga hot mot enskilda, men också mot samhället i stort. Skjutningar och sprängningar har i dagsläget ökat, ofta som en del i organiserad grov brottslighet, och det föreligger en förhöjd terrorhotnivå i Sverige. Detta innebär att ett större ingrepp i den personliga integriteten kan vara befogat till förmån för att ge de brottsbekämpande myndigheterna effektiva verktyg att genomföra sitt uppdrag.

11.2 En ny reglering för kamerabevakning på platser som allmänt används för trafik med motorfordon

När en plats dit allmänheten har tillträde kamerabevakas sker detta vanligen med stöd av kamerabevakningslagen. För de brottsbekämpande myndigheterna gäller inget krav på tillstånd för att få kamerabevaka sådana platser. Dock måste intresset av kamerabevakningen som utgångspunkt väga tyngre än den enskildes intresse av att inte bli bevakad. Ofta innebär detta att bevakning enbart får ske på en brottsutsatt plats. Vägar anses inte generellt utgöra en brottsutsatt plats. I betänkandet *Åtgärder i gränsnära*

områden (SOU 2021:92) anges att Polismyndigheten framfört att det är av stor betydelse för myndighetens verksamhet att kamerabevakning kan bedrivas på andra strategiskt viktiga platser och trafikleder i vägnätet utöver dem i gränsnära områden. Information från sådan bevakning kan ge myndigheten avgörande information i arbetet mot den organiserade brottsligheten. Sådan kamerabevakning skulle bl.a. kunna användas som ett system för att upptäcka rörelser av fordon eller personer kopplade till brottslig verksamhet. (Se a. SOU s. 211 och 337.)

Ett sätt att samla in uppgifter om fordon är genom kamerabevakning med ANPR-teknik (*automatic number plate recognition*). I dag används kamerabevakning med ANPR-teknik av bl.a. Polismyndigheten som ett verktyg i polisbilar och av Tullverket i gränskontroller. Uppgifter som samlas in genom kamerabevakning med ANPR-teknik är personuppgifter om fordon. För Polismyndighetens verksamhet har uppgifterna stor betydelse och kan användas för exempelvis följande syften.

- Lokalisera efterlysta personer och fordon,
- systematiskt omsätta underrättelser till operativ verksamhet genom informerade fordonsstopp baserat på aktuella bevakningar,
- utbyta information samt delta i den internationella samverkan genom att kunna lokalisera och vidta åtgärder mot internationellt kända eller efterlysta fordon,
- kartlägga fordon som förekommer i en brottsutredning och utreda nya brott som inte var kända vid tidpunkten för insamlingen,
- kartlägga fordon i underrättelseverksamheten som enligt redan kända underrättelser misstänks ha samband med brottslig verk-samhet,
- ge underlag för nya underrättelser om fordonsrörelser, individer, nätverk och modus kopplade till den organiserade och gräns-överskridande brottsligheten,
- ligga till grund för statistiska uppgifter som behövs i syfte att utveckla analysförmåga,

- upptäcka det som är okänt kopplat till den brottsliga verksamhet som undersöks genom analys av insamlat material samt
- genom insamlat material skapa beslutsunderlag för planering av underrättelsebaserat linjearbete, insatser och operationer, där Polismyndigheten oftare ska befinna sig på rätt plats vid rätt tid med rätt information, mot bakgrund av den uppgift som ska lösas.

Polismyndigheten har angett att myndighetens målbild med sin användning av uppgifter som har samlats in genom kamerabevakning med ANPR-teknik är att skapa en enhetlig och samlad förmåga som ska kunna tillhandahålla fordonsuppgifter och information om fordonsrörelser från utvalda strategiska platser i rätt tid och till rätt funktion. Syftet med användningen är att upptäcka, förebygga och förhindra brottslig verksamhet, utreda och lagföra brott samt upprätthålla säkerhet och ordning. Säkerhetspolisen har fört fram att myndighetens behov är i stort sett desamma som Polismyndighetens.

Intresset av att samla in och på andra sätt behandla information i syfte att förebygga, förhindra, utreda och lagföra brott får anses vara i hög grad berättigat, i synnerhet vad gäller den grova och organiserade brottsligheten. Behovet understryks bl.a. av det ökade antalet skjutningar och sprängningar. Sådan brottslighet kan få samhällshotande konsekvenser. Samhällsutvecklingen är således sådan att det får anses vara befogat att Polismyndigheten och Säkerhetspolisen ges möjlighet att använda de möjligheter som den moderna kamera- och igenkänningstekniken tillhandahåller för att förebygga, förhindra, utreda och lagföra allvarliga brott. Behovet måste dock tillgodoses på ett sätt som överensstämmer med bl.a. respekten för privatliv och skyddet för den personliga integriteten.

Uppgifter om fordon utgör som utgångspunkt personuppgifter. Dessa hör typiskt sett inte till de mer känsliga kategorierna av personuppgifter. Uppgifter om fordon kan normalt endast indirekt härledas till en fysisk person, det vill säga först genom jämförelse med uppgifter från andra källor. Uppgifterna kan alltså inte ensamma användas i syfte att identifiera en person. Så länge en identifierbar ansiktsbild på en förare eller passagerare inte samlas in

och bearbetas biometriskt utgör således uppgifter om fordon inte en känslig personuppgift enligt brottsdatalagens bestämmelser.

Vägar är platser där människor i betydande utsträckning förväntar sig att bli föremål för bevaknings- och kontrollåtgärder av olika slag. Trafikanter är i allmänhet medvetna om att det på vägar finns ett stort antal kameror för olika ändamål, t.ex. uttag av trängselskatt, automatisk hastighetskontroll och trafikövervakning. Det kan även tänkas finnas en beredskap och tolerans hos trafikanter att utsättas för kontroller på vägarna, bl.a. i form av fysiska poliskontroller men även i form av olika typer av automatiserade kontroller, med efterföljande användning av uppgifter om i vart fall deras motorfordon och hur fordonet har framförts.

11.2.1 Polismyndigheten och Säkerhetspolisen ska få bedriva kamerabevakning på platser som allmänt används för trafik med motorfordon utan att den föregås av en dokumenterad intresseavvägning

Förslag: Polismyndigheten och Säkerhetspolisen ges möjlighet att bedriva kamerabevakning på vägar, gator, torg och annan led eller plats som allmänt används för trafik med motorfordon utan krav på att en dokumenterad intresseavvägning ska göras innan kamerabevakningen påbörjas.

En förutsättning för att Polismyndigheten och Säkerhetspolisen ska få bedriva kamerabevakning är i de flesta fall att bevakningen föregås av en skriftligt dokumenterad intresseavvägning som visar att intresset av bevakningen väger tyngre än den enskildes intresse av att inte bli bevakad (14 a och 14 b §§ jämte 8 § kamerabevakningslagen). Kamerabevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning samt kamerabevakning som sker av vissa utpekade platser och i gränsnära områden är dock undantagna från kravet på dokumenterad intresseavvägning (14 c § 1–3 kamerabevakningslagen).

Vid bedömningen av intresset av kamerabevakning ska, enligt 8 § andra stycket kamerabevakningslagen, särskilt beaktas om bevakningen behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats eller på en annan plats där det av särskilt anledning finns risk för angrepp på någons liv, hälsa eller trygghet eller på egendom,
2. förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller begränsa verkningarna av sådana störningar,
3. utöva kontrollverksamhet,
4. förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor, eller
5. tillgodose andra därmed jämförliga ändamål.

Vid bedömningen av den enskildes intresse av att inte bli bevakad ska, enligt 8 § tredje stycket kamerabevakningslagen, särskilt beaktas

1. hur bevakningen ska utföras,
2. om teknik som främjar skyddet av den enskildes personliga integritet ska användas, och
3. vilket område som ska bevakas.

Det som föreskrivs i 8 § andra och tredje styckena kamerabevakningslagen är faktorer som Polismyndigheten har att beakta vid sin dokumenterade intresseavvägning. För att kamerabevakning ska få bedrivas måste det konkreta bevakningsintresset väga tyngre än integritetsintresset i det enskilda fallet. Bevakningsintresset kan skifta över tid och geografiskt område. Kriminalitetens omfattning och allvar är omständigheter som är av avgörande betydelse vid bedömningen av bevakningsintressets tyngd. I tider med allvarlig kriminalitet kan således balanspunkten mellan bevakningsintresset och den personliga integriteten förskjutas till nackdel för den personliga integriteten.

Brottsbekämpande myndigheter lägger inte sällan 8 § andra stycket 1 kamerabevakningslagen till grund för sin kamerabevakning. I punkten föreskrivs att det särskilt ska beaktas om bevakningen behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats eller på en annan plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet eller på egendom.

I dagsläget väger behovet av att bekämpa utvecklingen av grov organiserad brottslighet tungt. Med en brottsutsatt plats menas en plats där det finns problem med brottslighet (prop. 2017/18:231 s. 143). Det ospecifika begreppet brottsutsatt plats innebär en osäkerhet om vilka platser som faller in under begreppet. Denna osäkerhet kan medföra att tidskrävande analyser behöver göras inför en påbörjad kamerabevakning och kan leda till att kamerabevakning inte bedrivs i sådan utsträckning som lagen tillåter. Detta kan i sin tur leda till att brottsbekämpande myndigheter går miste om information som kan vara av avgörande betydelse i myndigheternas verksamhet.

I 8 § andra stycket 5 anges att behovet av att tillgodose andra ändamål som är jämförliga med de som anges i övriga punkter ska beaktas vid bedömningen om kamerabevakning behövs. Som exempel på sådana ändamål anges i förarbetena bevakning för att utföra en uppgift av betydelse för den nationella säkerheten som inte omfattas av de tidigare punkterna och inventering av djurbestånd eller annan viltvård (prop. 2017/18:231 s. 144). Spannet för vad som inryms under punkten är alltså stort. De fyra första punkterna skulle kunna betraktas som schablonbedömningar av det allmänna kravet på proportionalitet. När kamerabevakning sker för ett annat ändamål än de som framgår av dessa punkter kan det behöva göras mer ingående överväganden av behovet av kamerabevakning i förhållande till integritetsriskerna. Det kan även behöva vidtas särskilda åtgärder för att minska dessa risker (prop. 2017/18:231 s. 144).

Exempelvis olagliga transporter av människor och varor är en del i en allvarlig brottslig verksamhet. Transporterna sker ofta på vägar. I dagsläget föreligger en situation i Sverige där den organiserade grova brottsligheten ökar i omfattning och riskerar att få samhällshotande konsekvenser. Kamerabevakning av vägar som bedrivs av Polismyndigheten eller Säkerhetspolisen för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra grov brottslighet får utifrån dagens situation anses falla in under 8 § andra stycket 5 kamerabevakningslagen.

Polismyndigheten har fört fram att myndigheten ser ett behov av att i högre utsträckning kunna använda kamerabevakning med ANPR-teknik på vägarna. Att exempelvis kunna kombinera fasta ANPR-kameror med rörliga sådana möjliggör enligt Polis-

myndigheten ett effektivt informationsinhämtande och att den yttre verksamheten effektivt kan styras mot prioriterad brottslighet. Kamerabevakning med ANPR-teknik utgör en viktig komponent i arbetet att upptäcka, förebygga, förhindra och utreda såväl allvarlig och organiserad brottslighet som annan brottslighet. Enligt Polismyndigheten är det viktigt att en reglering som ger utökade möjligheter till kamerabevakning med ANPR-teknik inte blir för platsspecifik utan ger utrymme för en flexibilitet där myndighetens operativa behov får styra.

En utökad användning av kamerabevakning med ANPR-teknik innebär en viss ökning av intrång i den personliga integriteten. Omfattningen av den grova kriminaliteten i Sverige har emellertid nu nått en sådan nivå att det får anses befogat med ett större ingrepp i den personliga integriteten. Det föreslås att Polismyndigheten och Säkerhetspolisen ska få bedriva kamerabevakning på platser som allmänt används för trafik med motorfordon. De platser som avses är väg, gata, torg och annan led eller plats som allmänt används för trafik med motorfordon (jfr 2 § förordningen om vägtrafikdefinitioner). Förslaget innebär effektivare möjligheter för Polismyndigheten och Säkerhetspolisen att utföra sitt arbete då exempelvis kamerabevakning med ANPR-teknik kan bedrivas längs bl.a. vägar, vilket innebär bättre förutsättningar att följa olika, för myndigheterna intressanta, fordons färdväg. De integritetsförluster som en sådan ordning kan innebära kan vägas upp genom att det i polisens brottsdatalag regleras vilka personuppgifter som får samlas in genom kamerabevakning på platser som allmänt används för trafik med motorfordon samt hur uppgifterna får användas och hur länge de får lagras (se nedan avsnitt 11.2.2).

För att kamerabevakning med ANPR-teknik ska kunna användas effektivt på väg, gata, torg och annan led eller plats som allmänt används för trafik med motorfordon bör Polismyndigheten och Säkerhetspolisen undantas från kravet på att en intresseavvägning ska göras innan bevakningen påbörjas. På så sätt kan kamerabevakningen påbörjas snabbare när behovet uppstår. Eftersom de inledande skydds- och spaningsåtgärderna ofta är avgörande för utredningen av ett brott är det fördelaktigt för Polismyndigheten att snabbt och effektivt kunna ta del av uppgifter om brott som har inträffat i realtid.

Att Polismyndigheten och Säkerhetspolisen får bedriva kamerabevakning på platser som allmänt används för trafik med motorfordon utan att en intresseavvägning först görs innebär inte att bevakningen är oreglerad. Precis som med all kamerabevakning måste den, när den innebär en insamling av personuppgifter, ske i överensstämmelse med den dataskyddsrättsliga regleringen. När insamlingen sker för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd, upprätthålla allmän ordning och säkerhet eller fullgöra förpliktelser som följer av internationella åtaganden finns en rättslig grund för insamling av personuppgifter i 2 kap. 1 § polisens brottsdatalag. Utöver rättslig grund måste insamlingen ske för ett konkret ändamål i varje specifikt fall. Dataskyddsregleringen förutsätter att ändamålet med behandlingen av personuppgifter är definierat innan behandlingen påbörjas och regelverket tillåter inte att uppgiftssamlingar skapas för eventuella framtida behov.

Den föreslagna regleringen ger Polismyndigheten och Säkerhetspolisen möjlighet att bedriva insamling av personuppgifter som även rör personer som inte har någon koppling till brottslig verksamhet. Vid en sådan omfattande insamling av personuppgifter måste bl.a. en bedömning göras om insamlingen är proportionerlig och förenlig med principen om uppgiftsminimering. Att utforma en reglering som uppfyller syftet med lagändringen, det vill säga att förebygga, förhindra, upptäcka, utreda eller lagföra brott, på ett sätt som begränsar insamlingen av personuppgifter låter sig svårligen göras. En reglering som tillåter insamling av personuppgifter som inte tillgodoser syftet med insamlingen kan inte anses förenlig med dataskyddsregleringen. Den dataskyddsrättsliga regleringen innebär att det måste finnas ett konkret ändamål för varje specifik behandling av personuppgifter, vilket utgör en begränsning av hur insamling av personuppgifter genom kamerabevakning kan ske. Genom att det föreslås en begränsning av vilka personuppgifter som får användas samt för vilka ändamål och hur länge användningen får ske kan såväl syftet med regleringen uppnås som skyddet för den personliga integriteten tillgodoses (se avsnitt 11.2.2).

Nämnas bör även att det enligt 3 kap. 2 § brottsdatalagen ankommer på den personuppgiftsansvarige att genom lämpliga tekniska och organisatoriska åtgärder säkerställa att behandlingen av personuppgifter är författningsenlig och att den registrerades rättig-

heter skyddas. Av förarbetena till bestämmelsen (prop. 2017/18:232 s. 453) framgår att sådana organisatoriska åtgärder som avses i paragrafen bl.a. är att anta interna strategier för dataskydd, att informera och utbilda personalen och att säkerställa en tydlig ansvarsfördelning. Vilka åtgärder som bör vidtas får avgöras efter en bedömning i enskilda fall. Vid bedömningen har det betydelse bl.a. vilka personuppgifter som ska behandlas, mängden uppgifter och hur integritetskänsliga de är. Även grunden för behandlingen och riskerna med den ska beaktas. Mer långtgående åtgärder kan behövas vid behandling som kan medföra särskilda risker för integritetsintrång eller vid omfattande behandling av en stor mängd personuppgifter. Det ankommer alltså på Polismyndigheten och Säkerhetspolisen att vidta lämpliga åtgärder vid insamling av personuppgifter genom den föreslagna utvidgningen av myndigheternas möjlighet att använda sig av kamerabevakning med ANPR-teknik i syfte att minimera integritetsintrånget. Sådana åtgärder skulle exempelvis kunna vara inbyggt dataskydd genom maskering, att kamerorna är påslagna endast vissa tider och att enbart viss personal får tillgång till materialet. Det bör också beaktas att det kan behöva genomföras en konsekvensbedömning och ett förhandssamråd med tillsynsmyndigheten när kamerabevakning bedrivs enligt den föreslagna ordningen (se 3 kap. 7 § brottsdatalagen och 5 kap. 6 § säkerhetspolisens datalag).

11.2.2 En ny reglering om behandling av personuppgifter som samlats in av Polismyndigheten och Säkerhetspolisen genom kamerabevakning på platser som allmänt används för trafik med motorfordon

Förslag: För att väga upp den integritetsförlust som en utökning av möjligheterna till kamerabevakning innebär införs en begränsning av vilka personuppgifter som får användas samt för vilka ändamål och hur länge användningen får ske.

Personuppgifter som har samlats in genom kamerabevakning på platser som allmänt används för trafik med fordon och som rör motorfordon får behandlas av Polismyndigheten eller Säkerhetspolisen endast om syftet med behandlingen är att förebygga, förhindra, upptäcka, utreda eller lagföra brott för vilket det är föreskrivet fängelse i tre år eller mer. Sådan användning får alltid ske i sex månader efter det att uppgifterna samlades in. Detta ska inte gälla för personuppgifter i form av bilder av enskilda.

Den föreslagna regleringen innebär att en omfattande insamling kan ske av personuppgifter på väg, gata, torg och annan led eller plats som allmänt används för trafik med motorfordon. Det innebär att insamling kan ske av personuppgifter som rör personer som inte har någon koppling till brottslig verksamhet. Hur sådana personuppgifter får användas och lagras bör regleras tydligt i lag. Alltid när en personuppgift har samlats in måste användningen av uppgiften ske på ett sätt som är förenligt med dataskyddsregleringen, det måste bl.a. finnas en rättslig grund och ett berättigat ändamål för behandlingen. Eftersom kamerabevakning på platser som allmänt används för trafik med motorfordon regelbundet torde innebära att personuppgifter samlas in bör det införas regler som begränsar vilka personuppgifter som får användas, för vilket ändamål och hur länge de får lagras för att vara förenlig med skyddet för den personliga integriteten och dataskyddsregleringen, bl.a. principerna om uppgifts- och lagringsminimering och kraven på att behandlingen ska vara nödvändig och proportionerlig. En specifik rättslig grund bör införas i polisens brottsdatalag för Polismyndighetens och Säkerhetspolisens användning och lagring av personuppgifter som

samlats in genom kamerabevakning på platser som allmänt används för trafik med motorfordon.

Genom den föreslagna bestämmelsen om utökade möjligheter till kamerabevakning på platser som allmänt används för motortrafik kan olika typer av personuppgifter samlas in beroende på hur kamerabevakningen bedrivs. De personuppgifter som föreslås få användas med stöd av den föreslagna regleringen är uppgifter om motorfordon. Med motorfordon avses detsamma som i 2 § lagen (2001:559) om vägtrafikdefinitioner. Det kan bl.a. vara bilder på fordons registreringsskyltar med tillhörande uppgift om tid och plats för fordonets passage av kameran. Det kan även vara uppgifter om fordonets registreringsland och modell. En förutsättning för bestämmelsens tillämplighet är att uppgifterna utgör personuppgifter. Begreppet personuppgifter är avsett att ha samma innebörd som 1 kap. 6 § brottsdatalagen.

Med uppgifter om motorfordon avses inte sådana uppgifter som inte framgår av själva kamerabilden. Det kan bl.a. handla om ägaruppgifter som tas fram genom exempelvis vägtrafikregistret med hjälp av registreringsnummer. Sådana uppgifter samlas inte in genom kamerabevakningen utan på annat sätt (SOU 2021:92 s. 581). Med uppgifter om motorfordon avses inte heller bild på enskilda, det vill säga identifierbara förare eller passagerare i ett fordon. Att enbart uppgifter om motorfordon får användas med stöd av den föreslagna regleringen innebär ett mindre integritetsintrång och överensstämmer med vad som gäller för behandling av uppgifter från kamerabevakning i gränsnära områden (se 13 § lagen om polisiära befogenheter i gränsnära områden). Att insamlade uppgifter om motorfordon blir föremål för omfattande behandling kan anses vara mindre känsligt från integritetssynpunkt än behandling av många andra typer av personuppgifter (jfr prop. 2022/23:109 s. 40). För det fall Polismyndigheten eller Säkerhetspolisen vill använda andra personuppgifter i material från kamerabevakning på platser som allmänt används för trafik med motorfordon än motorfordon måste det ske med stöd av annan rättslig grund i tillämplig dataskyddsreglering.

Polismyndigheten har lyft fram ett behov av att kunna använda insamlade uppgifter från kamerabevakning i sin underrättelseverksamhet och framhållit att genom att analysera fordonsdata och mönster kan tidigare okända förhållanden om brottslighet

upptäckas. Det saknas anledning att betvivla att det finns en stor polisiär och operativ nytta med att t.ex. kunna sammanföra uppgifter om insamlade fordonsrörelser med uppgifter om motorfordon som underrättelseverksamheten bedömer ha samband med brottslig verksamhet, utan att det för den skull föreligger någon konkret brottsmisstanke. För att den nu föreslagna regleringen om kamerabevakning på platser som allmänt används för trafik med motorfordon ska vara förenlig med de dataskyddsrättsliga reglerna och skyddet för den personliga integriteten görs bedömningen att användningen av personuppgifter begränsas till ett visst ändamål. Ett sådant ändamål kan exempelvis vara att förebygga, förhindra, upptäcka, utreda eller lagföra brottsliga gärningar av viss svårhetsgrad.

Olika lösningar kan väljas när det kommer till att avgränsa vilka brott som ska kunna träffas av den föreslagna bestämmelsen. Det är angeläget att integritetsintrånget inte blir oproportionerligt i förhållande till de vinster som intrånget innebär för bekämpningen av den allvarliga brottsligheten. I sammanhanget kan nämnas lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen, som reglerar överföring och behandling av PNR-uppgifter (uppgifter om varje enskild passagerare som har lämnats vid bokning av en flygresa och vid incheckning) för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet. Lagen bygger på det s.k. PNR-direktivet[21]. Av 1 § fjärde stycket i den nyss nämnda lagen framgår att med annan allvarlig brottslighet avses i lagen de brott som anges i bilaga II till PNR-direktivet och för vilka det i Sverige eller andra medlemsstater är föreskrivet fängelse i tre år eller mer. Syftet med den nu föreslagna utvidgningen av kamerabevakning och lagen om flygpassageraruppgifter i brottsbekämpningen överensstämmer i allt väsentligt. Beaktas bör att det i den nämnda lagen är fråga om behandling av bl.a. resenärers namn, adress och kontaktuppgifter, fullständig resplan samt all betalnings- och bagageinformation, vilket får anses utgöra mer känsliga personuppgifter än fordonsuppgifter sett från en integritetssynpunkt.

[21] Europaparlamentets och rådets direktiv (EU) 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet.

En bestämmelse om hur personuppgifter som samlats in genom kamerabevakning på platser som allmänt används för trafik med motorfordon får användas bör föreskriva att användningen av insamlade uppgifter får avse personuppgifter som rör motorfordon samt att användning endast får ske om syftet med den är att förebygga, förhindra, upptäcka, utreda eller lagföra ett brott för vilka är föreskrivet fängelse i tre år eller mer. En sådan ordning innebär en teknikneutral bestämmelse som kan tillgodose användningen av personuppgifter i form av motorfordon som har samlats in på platser som allmänt används för trafik med motorfordon i Polismyndighetens och Säkerhetspolisens verksamhet samtidigt som skyddet för den personliga integriteten tillgodoses. Förslaget får anses falla inom gränserna för vad som kan anses vara nödvändig och proportionerlig användning av insamlade personuppgifter.

Beträffande den lagtekniska lösningen och placeringen av den nya föreslagna regeln görs följande överväganden. När brottsdatalagen infördes uttalade regeringen att utgångspunkten för lagens tillämpningsområde är att myndigheternas personuppgiftsbehandling i så stor utsträckning som möjligt ska regleras i respektive registerförfattning. En annan ordning, med enstaka bestämmelser om personuppgiftsbehandling i andra lagar, ansågs innebära att regleringen blir svåröverskådlig. (Se prop. 2017/18:269 s. 158.) Den bestämmelse som möjliggör behandling av personuppgifter om fordon såvitt gäller kamerabevakning i gränsnära områden har placerats i 13 § lagen om polisiära befogenheter i gränsnära områden. Bakgrunden till denna placering var att åstadkomma ett överskådligt regelverk och tydliggöra att bestämmelsen gäller just i gränsnära områden och ingen annanstans. (Se SOU 2021:92 s. 405.)

Regleringen om kamerabevakning på platser som allmänt används för trafik med motorfordon som föreslås får en generell geografisk giltighet och införandet av regleringen sker inte vid sidan av framtagandet av en helt ny lag för det specifika ändamålet. Det framstår därför som lämpligast att föra in en specifik reglering om rättslig grund gällande användandet av personuppgifter som samlats in genom kamerabevakning på platser som allmänt används för trafik med motorfordon efter den grundläggande bestämmelsen om rättslig grund för behandling av personuppgifter i 2 kap. 1 § polisens brottsdatalag.

Det bör, i likhet med bestämmelsen i 13 § lagen om polisiära befogenheter i gränsnära områden, framgå av lagtexten att bestämmelsen inte gäller uppgifter i form av bild av en enskild, det vill säga bild av identifierbara personer. För användning av sådana bilder måste stöd finnas i annan tillämplig dataskyddsrättslig reglering. I vilken utsträckning behandling av bilder av enskilda och andra personuppgifter som kan samlas in genom kamerabevakning på plats som allmänt används för trafik med motorfordon kan bedömas vara nödvändig och stå i proportion till de eventuella integritetsintrång som behandlingen innebär kan skifta kraftigt.

Tiden för användningen

I artikel 4.1 e dataskyddsdirektivet föreskrivs att personuppgifter inte ska förvaras i en form som möjliggör identifiering av den registrerade under längre tid än vad som är nödvändigt för de ändamål för vilka de behandlas. Det ska vidare enligt artikel 5 i direktivet föreskrivas lämpliga tidsgränser för radering av personuppgifter eller för periodisk översyn av behovet av att lagra personuppgifter. Dataskyddsdirektivet har i dessa delar genomförts genom bestämmelserna i 2 kap. 17 och 18 §§ brottsdatalagen och vissa bestämmelser om längsta tid för behandling i myndigheternas registerlagstiftning, bl.a. i 4 kap. polisens brottsdatalag.

I 2 kap. 17 § brottsdatalagen föreskrivs att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Av 4 kap. 2 § polisens brottsdatalag framgår att personuppgifter som inte har gjorts gemensamt tillgängliga inte får behandlas längre än ett år efter det att ärendet avslutades, om de behandlas i ett ärende, eller ett år efter det att de behandlades automatiserat första gången, om de inte kan hänföras till ett ärende. I 4 kap. 7–11 §§ finns bestämmelser om den längsta tid under vilken personuppgifter som har gjorts gemensamt tillgängliga får behandlas. Det kan i vissa fall bli aktuellt med kortare lagringstid än de tider som anges i 4 kap. polisens brottsdatalag, om det enligt den grundläggande regeln i 2 kap. 17 § brottsdatalagen inte bedöms nödvändigt att behandla en personuppgift så länge. Reglerna i 4 kap. polisens brottsdatalag är alltså just längsta tider, inte

minimitider under vilka det alltid ska anses nödvändigt och proportionerligt för polisen att behandla personuppgifter.

Den tidigare gällande kameraövervakningslagen, som år 2018 ersattes med den nuvarande kamerabevakningslagen, innehöll en uttrycklig bestämmelse om att bild- eller ljudmaterial från kamerabevakning av en plats dit allmänheten har tillträde som huvudregel fick bevaras under högst två månader. Att någon särskild tid för bevarande av kameramaterial i dag inte anges i lag kan dock inte utan vidare tolkas som att lagstiftaren avsett att en mer generös lagring av obearbetat videomaterial från kamerabevakning av en plats dit allmänheten har tillträde generellt sett skulle vara tillåten. Å andra sidan skulle det faktum att lagstiftaren valt att ta bort en tidigare gällande tidsgräns kunna indikera att det nu bör kunna vara möjligt att i större utsträckning göra olika bedömningar och att två månader inte längre är en självklar gräns. (Jfr SOU 2021:92 s. 374.)

Skälen för att tillåta att obearbetat videomaterial fick bevaras under två månader angavs i förarbetena till kameraövervakningslagen vara att det krävdes för att materialet skulle kunna användas exempelvis i brottsutredningar (prop. 2012/13:115 s. 123 f.). Detta är ett argument för lagring som fortsatt är aktuellt och relevant. I regel bör en lagringstid om i vart fall två månader därför kunna motiveras enligt gällande rätt avseende lagring av obearbetat videomaterial från kamerabevakning i allmänhet. Detta motsvarar den bedömning som gjordes beträffande bestämmelsen om lagring av personuppgifter som infördes i 13 § lagen om polisiära befogenheter i gränsnära områden. Utredningen ansåg att en lagringstid om sex månader utgjorde en balans mellan intresset av behandling av uppgifterna för brottsförebyggande och brottsbekämpande ändamål och skyddet för den personliga integriteten. Tiden ansågs tillgodose de brottsbekämpande myndigheternas behov, såväl inom underrättelseverksamheten som den brottsutredande verksamheten. Det konstaterades vidare att det har bedömts rimligt i andra sammanhang att obearbetat material får analyseras i sex månader för specifika ändamål. (Se SOU 2021:92 s. 394.)

Användning av personuppgifter under en längre tid än två månader kan, enligt dagens lagstiftning, anses tillåtet i de fall när uppgifterna blir föremål för vidare bearbetning eller analys i ett särskilt ärende med ett mer specificerat ändamål. Ett exempel på

sådan behandling kan vara om en uppgift om ett motorfordons registreringsnummer, som inhämtats genom att kamerabevakningsbilder bearbetats med ANPR-teknik, ger en ”träff” mot Polismyndighetens eller Säkerhetspolisens bevakningsregister eller annars är intressant inom ramen för en förundersökning. Behandlingen av personuppgifter sker då med stöd av bestämmelser i 4 kap. polisens brottsdatalag som innehåller lagringstider om minst ett år (jfr a. SOU s. 371 ff., 392 och 395).

Användning och lagring av personuppgifter om fordon som samlats in genom kamerabevakning på platser som allmänt används för trafik med motorfordon för de föreslagna ändamålen får bedömas vara nödvändig under längre tid än två månader för att tillgodose Polismyndighetens och Säkerhetspolisens behov, inte minst inom underrättelseverksamheten. Som framgått ovan får riskerna för intrång i den personliga integriteten anses vara mer begränsade vid användning av personuppgifter om motorfordon än de som föreligger vid behandling av personuppgifter som är direkt hänförbara till en identifierbar fysisk person. Detta eftersom fordonsuppgifter är av mindre integritetskänsligt slag. Om tiden för vilken lagring och behandling av uppgifter får ske är för kort hinner de brottsbekämpande myndigheterna inte bearbeta uppgifterna i tillräcklig utsträckning för att användningen ska fylla det syfte som ligger till grund för kamerabevakningen. Uppgifterna måste alltså få användas under en tillräckligt lång tid för att användningen ska vara meningsfull.

Polismyndigheten har lyft fram ett behov av att kunna behandla uppgifter från kamerabevakning bl.a. med ANPR-teknik under en tid av minst ett år. Det ifrågasätts inte att det kan finnas ett polisiärt behov av att få behandla material från kamerabevakning under så lång tid. En sådan lång lagringstid bedöms dock inte förenlig med den dataskyddsrättsliga principen om lagringsminimering. En lagringstid om ett år för så pass omfattande behandling av personuppgifter som den nu föreslagna utökningen av kamerabevakning innebär torde inte ha accepterats i några andra sammanhang som styrs av dataskyddsdirektivets reglering. Mot den bakgrunden görs bedömningen att det inte är möjligt att införa en reglering som tillåter att insamlade personuppgifter om fordon från kamerabevakning på plats som allmänt används för trafik med motorfordon får användas under ett år.

Av 13 § lagen om polisiära befogenheter i gränsnära områden framgår att personuppgifter som rör fordon och som har samlats in genom kamerabevakning i ett gränsnära område alltid får behandlas av bl.a. Polismyndigheten och Säkerhetspolisen i sex månader efter det att uppgifterna samlades in. En skillnad mellan den nu föreslagna regleringen och regleringen i lagen om polisiära befogenheter i gränsnära områden är att det geografiska tillämpningsområdet är väsentligt större i den här föreslagna regleringen. De risker för den personliga integriteten som den nu föreslagna regleringen innebär balanseras dock av att uppgifterna om motorfordon bara får användas för ett visst, begränsat ändamål. Detta ändamål är påtagligt mer begränsat än det för vilket fordonsuppgifter från kamerabevakning i gränsnära områden får användas, det vill säga att förebygga, förhindra, upptäcka, utreda eller lagföra brottslig verksamhet.

En möjlighet till användning av personuppgifter måste kunna godtas under i vart fall sex månader, om användningen begränsas till sådana personuppgifter och för sådant ändamål som nu föreslås. Det föreslås därför att personuppgifter om fordon som samlats in genom kamerabevakning på platser som allmänt används för trafik med motorfordon som ska användas för att förebygga, förhindra, upptäcka, utreda eller lagföra brott för vilket det är föreskrivet fängelse i tre år eller mer alltid ska få användas i sex månader efter det att de samlades in. Uppgifterna får användas så länge användningen sker för det konkreta ändamålet. Efter att den angivna tiden har gått ut, eller om användningen sker för andra ändamål, får möjligheten att använda uppgifterna avgöras med stöd av annan tillämplig dataskyddsrättslig reglering.

Det kan här noteras att s.k. PNR-uppgifter får behandlas i sex månader, vilket har bedömts vara förenligt med grundläggande dataskyddsrättsliga principer. Även denna reglering bygger på EU-rätt (PNR-direktivet). Den nu föreslagna regleringen har samma ändamål som behandlingen av PNR-uppgifter, det vill säga att bekämpa mycket allvarlig brottslighet.

Det kan även tilläggas att det kan finnas tekniska och praktiska aspekter som talar för att personuppgifter om fordon som samlats in genom kamerabevakning på plats som allmänt används för trafik med motorfordon får användas under samma tid som sådana uppgifter som är insamlade genom kamerabevakning i ett gränsnära

område. Det kan leda till tillämpningssvårigheter och utmaningar vad gäller tekniska lösningar och plattformar om uppgifter insamlade från olika delar av vägnätet får användas under olika tidsrymder. En lämpligare lösning för att åstadkomma en sådan differentiering som är sakligt påkallad och förenlig med dataskyddslagstiftningen är att i stället inskränka de ändamål för vilka de insamlade uppgifterna får användas.

11.3 Inget avskaffat krav på upplysning om kamerabevakning på platser som allmänt används för trafik med motorfordon

Bedömning: Det föreslås inte något ytterligare undantag från kravet på upplysning om kamerabevakning genom tydlig skyltning eller på något annat verksamt sätt enligt 15 § kamerabevakningslagen vid kamerabevakning på platser som allmänt används för trafik med motorfordon som bedrivs av Polismyndigheten eller Säkerhetspolisen.

Enligt 15 § första stycket kamerabevakningslagen ska en upplysning om kamerabevakning lämnas genom tydlig skyltning eller på något annat verksamt sätt. I andra stycket föreskrivs att om ljud kan avlyssnas eller tas upp vid bevakningen, ska en särskild upplysning lämnas om detta. Det vanligaste sättet att uppfylla kravet på upplysning är genom tydlig skyltning i direkt anslutning till den plats som kamerabevakas.

Från upplysningsplikten finns vissa undantag i 16 och 17 §§ kamerabevakningslagen. Av 16 § första stycket framgår bl.a. att upplysning om kamerabevakning och information om den personuppgiftsbehandling som kamerabevakningen innebär inte behöver lämnas vid bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning. Av 17 § framgår att tillsynsmyndigheten, om det finns synnerliga skäl, får besluta i enskilda fall om undantag från upplysningskravet och rätten till information om den personuppgiftsbehandling som kamerabevakningen innebär.

Polismyndigheten har framfört att det kan uppstå svårigheter för myndigheten att uppfylla kravet på skyltning när det kommer till

kamerabevakning i vägtrafiken. För att få sätta upp skyltar i anslutning till väg gäller vissa säkerhetsregler och en uppsättning av skylt kräver dessutom en samverkan med kommuner och Trafikverket. Det är också, enligt myndigheten, svårt att uppfylla det underliggande syftet med upplysningskravet vid kamerabevakning på vägar eftersom trafikanter får svårt att uppfatta den information som ska framgå på skylten. Polismyndigheten påpekar vidare att det är svårt att ge enskilda en möjlighet att justera sitt beteende för att undvika att bli bevakade, det vill säga välja en annan väg.

Av dessa skäl har Polismyndigheten bl.a. efterfrågat ett generellt undantag från kravet på skyltning vid kamerabevakning i vägtrafiken likt det som gäller när Polismyndigheten bedriver automatisk hastighetsövervakning. Polismyndigheten har betonat att det inte är fråga om att myndigheten vill bedriva dold kamerabevakning på vägarna. Det handlar om i vilken mån lagens regler är meningsfulla och genomförbara.

Frågan om utökade undantag från kravet på upplysning om kamerabevakning genom tydlig skyltning eller på något annat verksamt sätt har i närtid övervägts grundligt av 2023 års kamerabevakningsutredning i betänkandet *Kamerabevakning i offentlig verksamhet* (SOU 2024:27). Där föreslås inte något bredare undantag från upplysningskravet, bl.a. på den grunden att upplysningskravet och rätten till information utgör en möjlighet för den enskilde att tillvarata sina rättigheter i samband med kamerabevakning, och att utökade undantag således bör vara väl avgränsade (a. SOU s. 405 ff.).

Det har inte här framkommit att det skulle finnas några avgörande praktiska hinder mot att sätta upp skyltar vid de platser som allmänt används för trafik med motorfordon. De svårigheter som en eventuell samverkan med andra aktörer kan innebära kan av allt att döma bemästras. Som exempel kan nämnas att bl.a. Trafikverket i relativt stor utsträckning bedriver kamerabevakning längs de allmänna vägarna som omfattas av kamerabevakningslagens skyltningskrav. Kravet på upplysning är viktigt från integritetssynpunkt och möjliggör för enskilda att kunna välja om de vill bli föremål för kamerabevakning eller inte. En upplysning om att det bedrivs kamerabevakning på en plats är också viktig för ett effektivt brottsförebyggande.

Ett borttaget krav på att det ska lämnas en upplysning om kamerabevakning kan inte anses motsvara den vinst det ger för brottsbekämpande myndigheter när kamerabevakning bedrivs på platser som allmänt används för trafik med motorfordon. De undantag som i dag finns reglerade i kamerabevakningslagen tillkom bl.a. med hänvisning till att integritetsintrånget i de aktuella fallen är begränsat och att själva syftet med övervakningen skulle motverkas genom ett ovillkorligt krav på upplysning (se bl.a. prop. 1989/90:119 s. 30). Sådan kamerabevakning som föreslås få bedrivas på platser som allmänt används för trafik med motorfordon av Polismyndigheten och Säkerhetspolisen innebär ett intrång i den personliga integriteten eftersom regleringen möjliggör att en stor mängd personuppgifter samlas in. En skyltning om att kamerabevakning bedrivs kan i dessa fall inte heller anses motverka syftet med bevakningen. Det föreslås därför inte något undantag från kravet på att upplysning om kamerabevakning ska lämnas genom tydlig skyltning eller på något annat verksamt sätt när Polismyndigheten eller Säkerhetspolisen bedriver kamerabevakning på platser som allmänt används för trafik med motorfordon. Att en person som uppmärksammar skyltningen på en väg sällan har möjlighet att ta en annan väg utgör inte tillräckliga skäl för ett slopat krav om att upplysa om att kamerabevakning sker. Avsaknad av sådan skyltning gör det inte heller enklare för trafikanten i fråga att välja annan väg.

11.4 Polismyndigheten och Säkerhetspolisen får i vissa fall ges tillstånd att använda system för biometrisk fjärridentifiering i realtid på allmän plats för brottsbekämpningsändamål

Förslag: Polismyndigheten och Säkerhetspolisen ges möjlighet att i vissa fall få tillstånd att använda system för biometrisk fjärridentifiering i realtid på allmän plats för brottsbekämpningsändamål. Tillstånd ska få ges endast ges i den mån sådan användning är absolut nödvändig.

Möjligheten att identifiera personer med hjälp av biometri har utvecklats mycket snabbt på senare tid. Det gäller inte minst teknik för avancerad ansiktsigenkänning. Biometriska uppgifter utgör s.k. känsliga personuppgifter och behandling av sådana uppgifter är särskilt reglerad i det dataskyddsrättsliga regelverket. Av 2 kap. 12 § brottsdatalagen, samt 2 kap. 4 § och 6 kap. 4 § polisens brottsdatalag, framgår att biometriska uppgifter endast får behandlas om det är absolut nödvändigt för ändamålet med behandlingen. Regleringarna utgår från artikel 10 i dataskyddsdirektivet. Utvecklingen går mot att i allt större utsträckning använda AI för ansiktsigenkänning. Genom att dra nytta av den tekniska utvecklingen kan arbetet med att bekämpa organiserad brottslighet effektiviseras. Det är dock viktigt att den tekniska utvecklingen inte nyttjas på ett sätt som innebär oproportionerliga intrång i den enskildes personliga integritet och andra grundläggande fri- och rättigheter.

Den 13 mars 2024 antogs texten till den kommande EU-förordningen om AI[22]. Förordningen, som kommer bli direkt tillämplig i svensk rätt, bygger på en riskbaserad metod där olika AI-system regleras på olika sätt beroende på vilken risk systemet anses utgöra. Alla system för biometrisk fjärridentifiering anses utgöra högrisksystem och omfattas därför av strikta krav (se skäl 54).

I vissa avseenden innehåller förordningen bestämmelser som förutsätter eller ger utrymme för kompletterande nationella regler av olika slag. En sådan bestämmelse finns i artikel 5.5, där det framgår att en medlemsstat får föreskriva en möjlighet att helt eller delvis tillåta användning av system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpningsändamål inom vissa gränser och på vissa villkor. Det är alltså upp till respektive medlemsstat att, genom kompletterande lagstiftning i nationell rätt, ta ställning till om och på vilket sätt användning av sådana system ska få ske.

Biometrisk fjärridentifiering i realtid definieras som ett system för biometrisk fjärridentifiering där infångning av biometriska uppgifter, jämförelse och identifiering sker utan betydande dröjsmål

[22] Europaparlamentets ståndpunkt fastställd vid första behandlingen den 13 mars 2024 inför antagandet av Europaparlamentets och rådets förordning (EU) 2024/… om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (rättsakt om artificiell intelligens).

och omfattar inte bara omedelbar identifiering utan även begränsade korta fördröjningar för att undvika kringgående (artikel 3.42 AI-förordningen). Realtidssystem involverar direktupptagningar eller näst intill direktupptagningar av material, såsom videoupptagningar, genererade med kamera eller annan utrustning med liknande funktion. Efterhandssystem baseras däremot på redan insamlade biometriska uppgifter och jämförelsen och identifieringen sker med en betydande fördröjning. Detta involverar sådant material som bilder eller videoupptagningar som genereras genom bevakningskameror (CCTV) eller privat utrustning och som har genererats före användningen av systemet vad gäller de berörda fysiska personerna (se skäl 17).

Enligt artikel 5.5 AI-förordningen ska medlemsstaterna i sin nationella lagstiftning ange för vilka av de syften som förtecknas i artikel 5.1 h, inbegripet för vilka av de brott som avses i led iii i artikel 5.1 h, de behöriga myndigheterna kan få tillstånd att använda system för biometrisk fjärridentifiering i realtid för brottsbekämpningsändamål. Polismyndigheten har efterfrågat en möjlighet att få använda ansiktsigenkänning i realtid för att bl.a. eftersöka efterlysta personer för att kunna effektivisera sitt brottsbekämpande arbete.

Enligt artikel 5.1 h kan tillstånd att använda system för biometrisk fjärridentifiering i realtid endast ges i den mån sådan användning är absolut nödvändig för följande syften.

i. Målinriktad sökning efter specifika offer för människorov, människohandel eller sexuellt utnyttjande av människor, samt sökning efter försvunna personer.

ii. Förhindrande av ett specifikt, betydande och överhängande hot mot fysiska personers liv eller fysiska säkerhet eller ett verkligt och aktuellt eller verkligt och förutsebart hot om en terroristattack.

iii. Lokalisering eller identifiering av en person som misstänks ha begått ett brott, i syfte att genomföra en brottsutredning, lagföring eller ett verkställande av en straffrättslig påföljd för brott som avses i bilaga II och som i den berörda medlemsstaten kan leda till fängelse eller annan frihetsberövande åtgärd under en längsta tidsperiod på minst fyra år.

För att möta de behov som Polismyndigheten har lyft fram och för att möjliggöra effektiva sätt att förhindra potentiella terroristattacker samt hitta vissa brottsoffer bör Polismyndigheten och Säkerhetspolisen ges tillstånd att använda system för biometrisk fjärridentifiering i realtid för samtliga de syften som artikel 5.1 h AI-förordningen möjliggör. Det har inte framkommit att det finns ett behov för någon annan myndighet att få ges tillstånd till användning av sådana system. Användningen får ske inom Polismyndighetens verksamhet att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, eller upprätthålla allmän ordning och säkerhet samt i Säkerhetspolisens verksamhet gällande frågor som inte rör nationell säkerhet i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott (jfr 1 kap. 1 § polisens brottsdatalag och artikel 3.45 och 3.46 AI-förordningen).

Det framgår av artikel 5.3 i AI-förordningen att ett tillstånd, som huvudregel, måste lämnas i förväg för varje användning av system för biometrisk fjärridentifiering i realtid. Detta måste som utgångspunkt förstås som att tillståndet endast kan gälla en insats som är begränsad till tid och plats, och att någon av de förutsättningar som föreskrivs i artikel 5.1 h i–iii alltid måste vara för handen beträffande insatsen som helhet.

Gällande på vilka platser systemen får tillämpas används begreppet allmänt tillgänglig plats i AI-förordningen. Förordningens begrepp får anses stämma överens med begreppet allmän plats i den mening som det används i brottsbalken, det vill säga alla platser dit allmänheten har tillträde.

I förordningens artikel 5.1 h första punkten regleras bl.a. möjligheten att eftersöka offer för sexuellt utnyttjande av människor. Därmed ges stöd för att använda teknik för ansiktsigenkänning i realtid för att eftersöka offer för bl.a. barnpornografibrott och sådana brott som regleras i 6 kap. BrB.

Ett sådant hot mot fysiska personers liv eller fysiska säkerhet som avses enligt andra punkten kan vara följden av en allvarlig driftsstörning vid kritisk infrastruktur enligt definitionen i artikel 2.4 i Europaparlamentets och rådets direktiv (EU) 2022/2557[23], om en driftsstörning vid eller förstörelse av sådan infrastruktur skulle

[23] Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

leda till en omedelbar fara för en persons liv eller fysiska säkerhet, inbegripet genom allvarlig skada på tillhandahållandet av bas-förnödenheter till befolkningen eller på utövandet av statens kärnfunktion (skäl 33 AI-förordningen). Eftersom det enligt punkten ska vara ett övervägande och aktuellt hot ska det vara fråga om ett brådskande fall. Med begreppet terroristattack bör avses en sådan gärning som kan utgöra brott enligt 4 § terroristbrottslagen (2022:666).

De brott som omfattas av tredje punkten och som framgår av bilaga II i förordningen grundas på de 32 brott som förtecknas i rådets rambeslut 2002/584/RIF19[24]. Vid tillståndsförfarandet får en bedömning göras av om de brott som finns upptagna i bilagan har en motsvarighet i svensk rätt. Det föreskrivna straffet för brottet i svensk rätt måste vara fängelse i fyra år eller mer. Bedömningen är hänförlig till brottets straffskala och inte till en straffvärde-bedömning. En tydlig uppräkning av vilka brott som avses har inte ansetts nödvändig för att en reglering ska vara så tydlig och förutsebar att den lever upp till legalitetsprincipens krav (jfr prop. 2021/22:133 s. 77).

Artikel 5.1 h AI-förordningen föreskriver att brottsbekämpande myndigheter – utöver att användning av system för biometrisk fjärridentifiering i realtid endast får ske för något av de syften som anges – bara får ges tillstånd till användning av tekniken i den mån sådan är absolut nödvändig. En sådan begränsning tydliggör, likt bl.a. bestämmelserna i 2 kap. 12 § brottsdatalagen samt 2 kap. 4 § och 6 kap. 4 § polisens brottsdatalag, att det är fråga om undantagsfall som kräver ingående bedömningar om användningen verkligen är nödvändig då det handlar om behandling av känsliga person-uppgifter. Detta är en viktig begränsning för att skydda bl.a. den personliga integriteten. Tillstånd får vidare bara ges för brotts-bekämpningsändamål.

För att en regel som ger Polismyndigheten och Säkerhetspolisen möjlighet att använda teknik för ansiktsigenkänning i realtid ska kunna träda i kraft krävs att ytterligare bestämmelser införs. Det är fråga om bl.a. föreskrifter om vilken eller vilka myndigheter som ska vara marknadskontrollmyndighet till vilken varje användning av ett system för biometrisk fjärridentifiering i realtid på allmän plats ska

[24] Rådets rambeslut 2002/584/RIF av den 13 juni 2002 om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna.

anmälas och vilken rättslig eller oberoende administrativ myndighet som ska vara tillståndsgivare för sådana system (se artikel 5 punkterna 4 och 5 AI-förordningen). Det torde även behövas kompletterande bestämmelser som anger hur systemen och utdata från dessa får användas. Sådana bestämmelser är av stor vikt för att ge ett ytterligare skydd åt den personliga integriteten och andra grundläggande fri- och rättigheter.

Den föreslagna regleringen bör lämpligen föras in som en ny bestämmelse i polisens brottsdatalag eftersom det är fråga om tillstånd för insamling av personuppgifter som sker inom lagens tillämpningsområde.

11.5 Användning av teknik som extraherar information i bildmaterial från kamerabevakning

Bedömning: Användning av teknik som innebär att bildmaterial från kamerabevakning regelmässigt behandlas genom att viss information om innehållet i materialet extraheras kan inte anses förenlig med den dataskyddsrättsliga regleringen eller AI-förordningen.

Teknik som innebär att bild- och filmmaterial behandlas med AI-baserade bildanalysalgoritmer som extraherar viss information om innehållet i materialet kallas ibland för krunchning. Polismyndigheten har framhållit att myndigheten har ett behov av att mer regelmässigt kunna använda krunchning på bildmaterial från myndighetens bevakningskameror och från annans kamerabevakning som myndigheten får tillgång till. Syftet med krunchningen är att effektivisera användningen av den teknik som i dag finns tillgänglig. Polismyndigheten har framfört att myndigheten har ett behov av att kruncha bild- och filmmaterial redan vid insamlingen av materialet eftersom materialet då skulle kunna göras sök- och filtreringsbart direkt. På detta sätt skulle det kunna skapas sökbara databaser som exempelvis skulle kunna användas i nära tidsmässig anslutning till att ett brott begås.

Den hantering som krunchning innebär utgör en behandling av personuppgifter i form av biometriska uppgifter. Det är alltså fråga om behandling av sådana känsliga personuppgifter som Polis-

myndigheten och Säkerhetspolisen enligt 2 kap. 4 § polisens brottsdatalag får behandla endast om det är absolut nödvändigt för ändamålet med behandlingen. När kamerabevakning bedrivs är det ofta fråga om en omfattande insamling av personuppgifter. Det går att ifrågasätta om krunchning kan anses absolut nödvändig i förhållande till de kränkningar av de grundläggande rättigheterna som behandlingen ger upphov till sett i förhållande till ändamålet med behandlingen (jfr *EU-domstolens dom av den 26 januari 2023 V.S. mot Ministerstvo na vatreshnite raboti m.fl., C 205/21, EU:C:2023:49, p. 128-130*). Det är vidare tveksamt om det är förenligt med principen om uppgiftsminimering att utföra en sådan storskalig behandling av känsliga personuppgifter som krunchning av material från bevakningskameror i omedelbar anslutning till att materialet samlats in innebär.

Vidare måste reglerna i AI-förordningen beaktas. Eftersom krunchning inte innefattar något moment av jämförelse kan visserligen inte någon annan slutsats dras än att kruchning i och för sig inte innefattar någon biometrisk fjärridentifiering i realtid och således inte träffas av artikel 5.1 h i AI-förordningen. I artikel 5.1 e i förordningen föreskrivs emellertid att utsläppande på marknaden, ibruktagande för detta specifika ändamål eller användning av AI-system som skapar eller utvidgar databaser för ansiktsigenkänning genom oriktad skrapning av ansiktsbilder från internet eller övervakningskameror är förbjudet. Av skäl 43 framgår att sådana nämnda metoder ökar känslan av att det förekommer mass-övervakning och kan leda till grova kränkningar av grundläggande rättigheter, inbegripet rätten till integritet.

Vad begreppet skrapning innebär enligt artikel 5.1 e i AI-förordningen är inte helt klart. Utifrån hur begreppet används i förordningen får det dock anses innebära att information extraheras automatiskt eller med hjälp av en dator ur en bild. Med oriktad skrapning måste anses menas att skrapningen inte är inriktad på bilder av en viss person, utan att extrahering av information sker från bilder i ett obestämt material. Vid kamerabevakning styr vanligen händelseförlopp på platsen där bevakningen bedrivs vilket bildmaterial som samlas in. Det får därmed anses vara fråga om insamling av ett obestämt material. Behandling i form av krunchning av ett bildmaterial från kamerabevakning kan alltså inte anses förenligt med artikel 5.1 e AI-förordningen. Det föreslås därför

ingen reglering som möjliggör regelmässig användning av krunchning.

11.6 En utvidgad uppgiftsskyldighet för Transportstyrelsen avseende uppgifter från trängselskattekameror och infrastrukturavgiftskameror

Förslag: Transportstyrelsen ska på begäran av Polismyndigheten eller Säkerhetspolisen utan dröjsmål lämna ut uppgifter om trängselskatt eller infrastrukturavgift som gäller passager av en betalstation eller kontrollpunkt om det av begäran framgår att uppgifterna behövs i ett brådskande fall för att förebygga, förhindra, upptäcka eller utreda ett brott för vilket det är föreskrivet fängelse i tre år eller mer eller ett straffbart försök eller en straffbar förberedelse eller stämpling till eller underlåtenhet att avslöja eller förhindra sådant brott.

Polismyndigheten har framhållit att myndigheten har ett operativt intresse av att i större utsträckning kunna ta del av material från trängselskattekameror. Myndigheten har även framfört ett behov av att på ett snabbt sätt kunna ta del av material från kameror som är uppsatta för att ta ut infrastrukturavgift. Eftersom de inledande skydds- och spaningsåtgärderna ofta är avgörande för utredningen av ett brott är det fördelaktigt för Polismyndigheten att snabbt och effektivt kunna ta del av uppgifter om brott som har inträffat i realtid. Detta bl.a. för att identifiera en gärningsperson och för att förhindra att ytterligare brott inträffar. Samma sak gäller när en brottsbekämpande myndighet har underrättelser som tyder på att ett brott planeras eller är nära förestående (se även SOU 2023:69 s. 645).

När systemet med trängselskatt infördes lades under lagstiftningsprocessen stor vikt vid integritetsaspekten. Bland annat uttalade regeringen i förarbetena att det är angeläget att den enskildes integritet värnas så långt som möjligt. Möjligheten att kartlägga en persons förflyttningar in i och ut ur ett område som omfattas av trängselskatt skulle därför, enligt regeringen, omfattas av sekretess. (Se prop. 2003/04:145 s. 90 och 102 f.) Motsvarande

överväganden och uttalanden gjordes knappt tio år senare när systemet med infrastrukturavgifter infördes. I samband med detta uttalade även regeringen att de överväganden som gjordes vid införandet av systemet med trängselskatt enligt regeringens uppfattning fortfarande var relevanta (prop. 2013/14:25 s. 77 f.).

Enligt 27 kap. 1 § första stycket OSL föreligger absolut sekretess för uppgift om en enskilds personliga eller ekonomiska förhållanden bl.a. i en verksamhet som avser bestämmande av skatt. I verksamhet som avser bestämmande av infrastrukturavgift på väg, avgift med anledning av att infrastrukturavgift inte har betalats i rätt tid eller fastställande av underlag för bestämmande av sådana avgifter gäller 29 kap. 5 a § OSL. Precis som skattesekretessen gäller absolut sekretess för uppgifter om enskilds personliga eller ekonomiska förhållanden i verksamhet som avser infrastrukturavgift.

Av 10 kap. 28 § OSL framgår att sekretess inte hindrar att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. En sådan uppgiftsskyldighet finns i 5 kap. 3 a § vägtrafikdataförordningen (2019:382). Enligt bestämmelsen ska Transportstyrelsen på begäran av Polismyndigheten eller Säkerhetspolisen utan dröjsmål lämna ut uppgifter om trängselskatt som gäller passager av en betalstation eller kontrollpunkt om det av begäran framgår att uppgifterna i ett brådskande fall behövs för att förhindra eller på annat sätt ingripa mot en handling som kan utgöra terroristbrott enligt 4 § terroristbrottslagen (2022:666) eller försök, förberedelse eller stämpling till eller underlåtenhet att avslöja eller förhindra sådant brott.

Gällande infrastrukturavgift finns ingen reglerad uppgiftsskyldighet som den i 5 kap. 3 a § vägtrafikdataförordningen. Uppgifter om infrastrukturavgift kan, i likhet med uppgifter om trängselskatt som behövs för att förhindra eller ingripa mot andra brott än potentiella terroristbrott, i stället lämnas ut till Polismyndigheten och Säkerhetspolisen med tillämpning av 10 kap. 24 och 27 §§ OSL. Även om Transportstyrelsen torde ha stöd i bestämmelserna för att lämna ut uppgifter om såväl infrastrukturavgifter som trängselskatt i andra fall än de som omfattas av uppgiftsskyldigheten till Polismyndigheten eller Säkerhetspolisen i nämnda situationer måste ett utlämnande alltid föregås av en sekretessprövning. Bestämmelserna kan alltså inte

läggas till grund för ett löpande eller mer rutinmässigt utlämnande och kan därmed inte tillgodose Polismyndighetens och Säkerhetspolisens behov i de mest brådskande fallen.

Ett möjligt sätt att tillmötesgå Polismyndighetens identifierade behov är att utvidga tillämpningsområdet för 5 kap. 3 a § vägtrafikdataförordningen till att gälla vid fler brott. En sådan utvidgad uppgiftsskyldighet måste dock vara proportionerlig i förhållande till det integritetsintrång som utvidgningen innebär. Vid denna bedömning måste bl.a. beaktas vilken karaktär de uppgifter som kan komma att omfattas av uppgiftsskyldigheten har. Kameror vid betalstationerna för trängselskatt och infrastrukturavgift är inställda på så sätt att enbart registreringsnumret på passerande fordon ska läsas av. Viss överskottsinformation kan registreras, som t.ex. den del av fordonet som är närmast registreringsskylten, men de aktuella kamerorna tar inte bild på personer som färdas i fordonet. Enbart uppgifter från en kamera vid en betalstation kan därför inte användas för att kartlägga en persons rörelsemönster. Uppgifter om fordon, inklusive uppgifter om när fordon passerar en kamera, anses typiskt sett inte vara känsliga personuppgifter. Vägar är inte heller platser där personer uppehåller sig i någon större utsträckning annat än som transportsträcka mellan två platser, vilket också gör uppgifterna mindre känsliga från integritetssynpunkt.

Ett förslag om att utvidga tillämpningsområdet för 5 kap. 3 a § vägtrafikförordningen har lämnats i betänkandet *Ökat informationsflöde till brottsbekämpningen* gällande trängselskattekameror (SOU 2023:69). I betänkandet föreslås att Transportstyrelsen ska vara skyldig att lämna ut uppgifter från trängselskattekameror till Polismyndigheten, Säkerhetspolisen eller Tullverket när de behövs i ett brådskande fall för att förebygga, förhindra, upptäcka eller utreda en handling som kan utgöra brott för vilket det i straffskalan ingår fängelse i ett år eller mer, eller ett straffbart försök eller en straffbar förberedelse eller stämpling till eller underlåtenhet att avslöja eller förhindra sådant brott. Förslaget är under behandling i Regeringskansliet och har i dagsläget inte lett till någon ändring i förordningen.

En utvidgning som är mer begränsad än den som föreslagits i ovan nämnda betänkande är att Transportstyrelsen ska vara skyldig att lämna ut uppgifter till Polismyndigheten eller Säkerhetspolisen när det behövs för att förebygga, förhindra, upptäcka eller utreda brott

för vilket det är föreskrivet fängelse i tre år eller mer. I likhet med beträffande terroristbrott får det anses finnas ett starkt samhälleligt intresse av att förebygga, förhindra, upptäcka eller utreda sådana brott. Inte minst i dagsläget där situationen är sådan att våldsbrott och skjutningar ökar i samhället. Polismyndighetens och Säkerhetspolisens intresse får i dessa mer allvarliga fall som utgångspunkt anses väga tyngre än den enskildes intresse av att passera en trängselskattekamera eller infrastrukturavgiftskamera utan att det ska komma till brottsbekämpande myndigheters kännedom. Genom att begränsa uppgiftsskyldigheten till att enbart gälla brott för vilket det är föreskrivet fängelse i tre år eller mer kan skyddet av den enskildes personliga integritet tillgodoses på ett balanserat sätt i förhållande till Polismyndighetens och Säkerhetspolisens behov av en enklare och mer enhetlig hantering av utlämnande av uppgifter från kameror i de brådskande fallen.

Den föreslagna regleringen innebär att uppgiftsskyldigheten även ska gälla för material från infrastrukturavgiftskameror. I dagsläget finns betalstationer för infrastrukturavgifter försedda med kameror uppsatta på tre platser i Sverige. Kamerorna samlar in samma typ av personuppgifter som trängselskattekamerorna, det vill säga uppgifter om fordon. Kamerorna är dock påslagna dygnet runt och genererar därmed fler bilder än trängselskattekamerorna. I likhet med skattesekretessen gäller absolut sekretess för uppgifter om infrastrukturavgift. Den sekretess som blir tillämplig hos mottagande myndigheter när uppgifter från kamerorna lämnas ut är visserligen något svagare, men får anses ge ett tillräckligt skydd (se bl.a. 18 kap. 1 §, 35 kap. 1 § och 32 kap. 3 § OSL). En uppgiftsskyldighet som även omfattar material från kameror vid betalstationer för infrastrukturavgift kan inte anses innebära att personuppgiftsbehandlingen går utöver vad som är nödvändigt med hänsyn till syftet med den föreslagna ändringen.

Det är upp till Polismyndigheten eller Säkerhetspolisen att avgöra om det föreligger en sådan situation som bestämmelsen omfattar innan en begäran om utfående av uppgifter görs.

11.7 Uppgifter från kamerabevakning ska kunna göras gemensamt tillgängliga

Förslag: Uppgifter som samlats in genom kamerabevakning med stöd av kamerabevakningslagen (2018:1200) eller annan författning ska få göras gemensamt tillgängliga. Tillgången till sådana uppgifter ska begränsas till särskilt angivna tjänstemän som är i behov av uppgifterna för att upprätthålla allmän ordning och säkerhet eller förebygga, förhindra, upptäcka eller utreda och lagföra ett brott för vilket är föreskrivet fängelse i tre år eller mer.

Polismyndigheten bedriver kamerabevakning på flera olika sätt, bl.a. med fasta och tillfälliga egna kameror, samt i samverkan med externa aktörer. En stor del av det kameramaterial som Polismyndigheten har tillgång till lagras i myndighetens nationella kameraplattform. Polismyndigheten har framfört att det råder oklarheter kring om det finns laglig grund att göra personuppgifter som inhämtats genom kamerabevakning gemensamt tillgängliga.

Möjligheterna att göra personuppgifter gemensamt tillgängliga i Polismyndighetens och i vissa fall Säkerhetspolisens verksamhet regleras i 3 kap. 2 § polisens brottsdatalag. Bestämmelsen reglerar sådan behandling av uppgifter som sker i för verksamheten gemensamma uppgiftssamlingar. Med gemensamt tillgängliga uppgifter avses inte sådana uppgifter som endast ett fåtal personer har rätt att ta del av (3 kap. 1 § första stycket polisens brottsdatalag). En tumregel för hur många personer som avses med ett fåtal är ett tiotal (prop. 2009/10:85 s. 128 f.).

Av 3 kap. 2 § första stycket polisens brottsdatalag framgår att uppgifter får göras gemensamt tillgängliga om de kan antas ha samband med misstänkt brottslig verksamhet, under förutsättning att den misstänkta verksamheten innefattar brott för vilket det är föreskrivet fängelse i ett år eller mer eller sker systematiskt (punkten 1) samt om de behövs för övervakningen av en person som kan antas komma att begå brott för vilket det är föreskrivet fängelse i två år eller mer och är allvarligt kriminellt belastad eller kan antas utgöra ett hot mot andras personliga säkerhet (punkten 2). Dessa två punkter motsvarar de som tidigare fanns i 3 kap. 2 § första stycket 1 och 2 polisdatalagen (2010:361).

Av förarbetena till polisdatalagen framgår att personuppgifter enligt punkterna 1 och 2 får göras gemensamt tillgängliga i polisarbete som avser att förebygga, förhindra eller upptäcka brottslig verksamhet (prop. 2009/10:85 s. 131–136). Begreppet förebygga, förhindra eller upptäcka brott innefattar all egentlig brottsbekämpande verksamhet inom Polismyndigheten som inte direkt kan knytas till en brottsutredning, däribland behandling i myndighetens underrättelseverksamhet och där det inte finns någon misstanke om ett konkret brott (a. prop. s. 102 ff.). När polisens brottsdatalag infördes framhöll regeringen att begreppet förebygga, förhindra eller upptäcka brott är avsett att ha samma betydelse som i polisdatalagen. Bestämmelsen i polisens brottsdatalag om vilka personuppgifter som får göras gemensamt tillgängliga motsvarar de som gällde i polisdatalagen, med den skillnaden att två nya punkter tillkom. (Se prop. 2017/18:269 s. 294 och 300 f.)

Av 3 kap. 2 § polisens brottsdatalag första stycket 7 framgår att uppgifter som behandlas i syfte att upprätthålla allmän ordning och säkerhet får göras gemensamt tillgängliga. I förarbetena till polisdatalagen framhölls att det är svårt att dra en tydlig gräns mellan polisens ordningshållning och brottsbekämpning, vilket beror på att övervakning och ordningshållande verksamhet även kan syfta till att förebygga och ingripa mot brott. Sådan verksamhet kan också ofta övergå i brottsbekämpning (se prop. 2009/10:85 s. 75). I förarbetena till polisens brottsdatalag framgår vidare att det kan finnas behov av att göra uppgifter om tillträdesförbud eller uppgifter om personer som tidigare orsakat ordningsstörningar gemensamt tillgängliga inför kommenderingar vid särskilda händelser där ordningsstörningar befaras, t.ex. en fotbollsmatch eller en demonstration. Regeringen uttalade att det inte var givet att sådana uppgifter alltid kunde göras gemensamt tillgängliga med stöd av befintlig reglering. (Se prop. 2017/18:269 s. 163.) Bestämmelsen ger en generell möjlighet att göra personuppgifter tillgängliga utan någon kontroll av om den som personuppgiften rör är registrerad i underrättelseverksamheten, är misstänkt för brott eller förekommer i något annat sammanhang som ger möjlighet att göra personuppgifterna gemensamt tillgängliga (a. prop. s 301).

Även vissa uppgifter om personer som inte misstänks för delaktighet i brottslig verksamhet får göras gemensamt tillgängliga. Detta gäller exempelvis uppgifter om den som har informerat

Polismyndigheten om den misstänkta brottsliga verksamheten, om en person som äger ett garage eller annan lokal där den misstänkta brottsliga verksamheten bedrivs, om anhöriga eller andra som genom sitt samröre med den misstänkte kan vara av intresse i underrättelsearbetet samt uppgifter om att en bevakad person är anställd hos en viss annan person eller att den bevakade personen regelbundet besöker vissa personer. En förutsättning är att uppgifterna har koppling till misstänkt brottslig verksamhet eller att det finns ett behov av uppgifterna för övervakning av vissa personer. För att skydda den enskildes integritet i dessa fall finns bl.a. bestämmelser som förhindrar att uppgifterna ges omotiverad spridning. (Se prop. 2009/10:85 s. 135 f. och 138.)

Polismyndigheten och Säkerhetspolisen behöver på ett effektivt sätt kunna nyttja information som samlats in genom kamerabevakning. Material från kamerabevakning lagras i dag till stor del i en nationell kameraplattform hos Polismyndigheten. En del i ett effektivt nyttjande av information är att den ska kunna göras gemensamt tillgänglig så att det finns ett informationsflöde inom myndigheterna. I många fall kan vissa personuppgifter som samlas in genom kamerabevakning göras gemensamt tillgängliga bl.a. med stöd av ovan nämnda punkter i 3 kap. 2 § polisens brottsdatalag. När kamerabevakning bedrivs samlas stora mängder uppgifter in. Det är oundvikligt att insamlingen omfattar överskottsinformation. Sådan kan svårligen separeras från uppgifter som är relevanta för det ändamål som kamerabevakningen bedrivs. Detta innebär att Polismyndigheten och Säkerhetspolisen kan behöva behandla uppgifter som rör personer som inte kan knytas till någon av de befintliga punkterna i 3 kap. 2 § polisens brottsdatalag när myndigheterna behandlar uppgifter från kamerabevakning för olika ändamål. Ett informationsflöde behöver regleras för att värna den enskildes integritet då det är fråga om en omfattande mängd personuppgifter som bl.a. kan röra personer utan koppling till ändamålet med kamerabevakningen.

Bestämmelserna i polisens brottsdatalag om när uppgifter får göras gemensamt tillgängliga tar genomgående sikte på olika situationer när uppgifterna behövs i ett specifikt ärende. I motiven till polisdatalagen anges att begreppet ärende där hade en särskild innebörd som kan avvika från den gängse innebörden av begreppet i den då gällande förvaltningslagen (1986:223). Med ärende avsågs en

serie åtgärder som är avsedda att leda fram till ett bestämt slut. Särskilda underrättelseprojekt kunde t.ex. omfattas. Underrättelseprojekt med en obestämd varaktighet, exempelvis ett projekt som syftar till att fortlöpande undersöka ungdomsbrottsligheten på en viss ort, ansågs dock inte som ett ärende i den mening som avsågs i paragrafen. (Se prop. 2009/10:85 s. 328.) När det gäller organiserad brottslighet och grova våldsbrott finns det ett behov av att uppgifter får göras gemensamt tillgängliga i bl.a. underrättelseverksamheten utan att det finns ett specifikt ärende upplagt eller att materialet har strukturerats.

Bestämmelsen i 3 kap. 2 § polisens brottsdatalag har till syfte att motverka risken för otillbörliga intrång i den personliga integriteten när personuppgifter behandlas av eller är tillgängliga för fler än ett fåtal personer och samtidigt ge Polismyndigheten och Säkerhetspolisen nödvändigt utrymme att behandla personuppgifter för att förebygga, förhindra, upptäcka eller utreda och lagföra brott samt upprätthålla allmän ordning och säkerhet. Ett sätt att tillgodose båda dessa behov är att möjliggöra att uppgifter från kamerabevakning får göras gemensamt tillgängliga för dessa ändamål men att tillgången till sådana uppgifter begränsas. En sådan begränsning finns bl.a. i 3 kap. 2 § tredje stycket polisens brottsdatalag som föreskriver att endast särskilt angivna tjänstemän som har till uppgift att arbeta med övervakningen får ges tillgång till uppgifter som har gjorts gemensamt tillgängliga med stöd av första stycket 2.

Det får anses finnas ett behov av att möjliggöra att uppgifter i bl.a. Polismyndighetens nationella kameraplattform får göras gemensamt tillgängliga. Mot bakgrund av det stora antalet personuppgifter som material från kamerabevakning ofta innehåller bör det införas en begränsning av den personkrets som får tillgång till uppgifterna. Det föreslås att en ny reglering införs i polisens brottsdatalag som föreskriver att personuppgifter som samlats in genom kamerabevakning får göras gemensamt tillgängliga. Bestämmelsen innebär att allt material som samlats in genom kamerabevakning med stöd av kamerabevakningslagen eller annan författning får göras gemensamt tillgängliga. Detta innebär att även sådant material som inte härrör från kamerabevakning som Polismyndigheten eller Säkerhetspolisen bedriver men som är tillgängligt för dessa myndigheter kan göras gemensamt tillgängligt. Tillgången till sådant material bör dock begränsas till särskilt angivna tjänstemän som är i

behov av uppgifterna för att upprätthålla allmän ordning och säkerhet eller förebygga, förhindra, upptäcka eller utreda och lagföra ett brott för vilket är föreskrivet fängelse i tre år eller mer. Genom att begränsa tillgången till uppgifterna minskar risken för otillbörliga intrång i den personliga integriteten. Till detta kommer bl.a. bestämmelsen om sökbegränsningar i 3 kap. 5 § polisens brottsdatalag som ytterligare tillgodoser skyddet för den personliga integriteten genom att möjligheten att kartlägga enskildas personliga förhållanden begränsas. Det ankommer på Polismyndigheten och Säkerhetspolisen att organisera sin verksamhet på ett sådant sätt att obefogad spridning av personuppgifter motverkas samt säkerställa att det finns tekniska begränsningar i bl.a. den nationella kameraplattformen och att slagningar i denna loggas m.m.

I sammanhanget kan noteras att den s.k. PNR-lagstiftningen, som härrör från EU-rätt, innehåller en uttrycklig reglering om insamling och fortsatt behandling av en omfattande mängd personuppgifter avseende personer som till största del inte är misstänkta för brott, nämligen flygpassageraruppgifter. Möjligheten är begränsad till att gälla endast för mycket allvarlig brottslighet, likt sådan som den föreslagna bestämmelsen tar sikte på. Den föreslagna regleringen får anses vara nödvändig och proportionerlig.

Direktåtkomst

Genom att uppgifter som samlats in genom kamerabevakning görs gemensamt tillgängliga blir även bestämmelsen i 3 kap. 7 § polisens brottsdatalag tillämplig. Där föreskrivs att Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket får medges direktåtkomst för ett syfte som anges i 1 kap. 2 § brottsdatalagen (2018:1177) till personuppgifter som har gjorts gemensamt tillgängliga enligt 3 kap. 2 § polisens brottsdatalag. Ett effektivt och framgångsrikt arbete mot allvarlig och organiserad brottslighet förutsätter att man kan dra nytta av den samlade kunskap om brott som finns inte bara inom olika delar av polisorganisationen utan också hos andra brottsbekämpande myndigheter. Av samma skäl som det är viktigt att man inom Polismyndigheten på ett effektivare sätt kan tillgodogöra sig den information som finns inom den egna

organisationen, är det viktigt att nyttiggöra informationen i samarbetet med andra brottsbekämpande organ. Det är också en strävan inom EU att öka informationsutbytet mellan medlemsstaternas brottsbekämpande myndigheter (jfr bl.a. PNR-direktivet[25]). (Se prop. 2009/10:85 s. 166 f.)

Vid informationsutbyte mellan brottsbekämpande myndigheter bör beaktas att de myndigheter som bedriver underrättelseverksamhet har likartade regler om sådan verksamhet och att alla myndigheter tillämpar samma grundläggande regler för brottsutredning. Vidare har uppgifter som rör brott och brottsbekämpning samma sekretesskydd hos alla berörda myndigheter. Skyddet vid personuppgiftsbehandling är också likartat. (Se a. prop. s. 167.) En bestämmelse om direktåtkomst reglerar endast formen för utlämnande av uppgifter. Regleringen i 3 kap. 7 § polisens brottsdatalag är alltså inte sekretessbrytande och direktåtkomst kan därför endast medges till uppgifter som inte omfattas av sekretess.

Det finns en sekretessbrytande bestämmelse i 2 kap. 8 § polisens brottsdatalag som möjliggör för Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Kustbevakningen och Tullverket att, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 § OSL, ta del av personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § polisens brottsdatalag, om den mottagande myndigheten behöver uppgifterna för ett syfte som anges i 1 kap. 2 § brottsdatalagen. Bestämmelsen är utformad som en uppgiftsskyldighet (se prop. 2009/10:85 s. 331). Uppgift om enskildas personliga förhållanden som samlats in genom kamerabevakning omfattas enligt 32 kap. 3 § OSL av sekretess, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. Genom den sekretessbrytande bestämmelsen i 32 kap. 3 a § OSL får sådana uppgifter lämnas ut till vissa angivna brottsbekämpande myndigheter om de behövs för att utreda ett begånget brott för vilket fängelse är föreskrivet eller för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket fängelse är föreskrivet.

[25] Europaparlamentets och rådets direktiv (EU) 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet.

Ju fler personer som har omedelbar tillgång till personuppgifter, desto mer påtaglig är risken för intrång. Direktåtkomst kan också minska möjligheterna att kontrollera den vidare användningen av uppgifterna. De ökade integritetsrisker som en möjlighet till direktåtkomst kan medföra kan dock motverkas genom bestämmelser av annat slag, såsom befintliga bestämmelser om sekretess hos den mottagande myndigheten och bestämmelser om tillgång till uppgifter och om informationssäkerhet (jfr prop. 2009/10:85 s. 176 f.). Det ska i sammanhanget beaktas att vid direktåtkomst överförs vanligen sekretessen hos den myndigheten som uppgiften finns hos till den mottagande myndigheten (se 11 kap. 4 § OSL). Vid direktåtkomst har samma begränsning om tillgång till personuppgifter ansetts gälla hos den mottagande myndigheten (a. prop. s. 177). Detta innebär att endast tjänstemän hos den mottagande myndigheten som behöver uppgifter för att förebygga, förhindra, upptäcka eller utreda och lagföra ett brott för vilket är föreskrivet fängelse i tre år eller mer ska kunna få tillgång till uppgifterna.

11.8 Längsta tid för behandling av gemensamt tillgängliga uppgifter som samlats in genom kamerabevakning

Förslag: Personuppgifter som samlats in genom kamerabevakning enligt reglerna i kamerabevakningslagen (2018:1200) eller annan författning och som gjorts gemensamt tillgängliga med stöd av den föreslagna bestämmelsen i punkt 9 i 3 kap. 2 § första stycket polisens brottsdatalag får inte behandlas längre än sex månader efter det att de samlades in.

Det föreslås att en bestämmelse införs om att personuppgifter som samlats in genom kamerabevakning med stöd av kamerabevakningslagen (2018:1200) eller annan författning ska få göras gemensamt tillgängliga för vissa ändamål. I och med detta aktualiseras frågan hur länge uppgifterna ska få behandlas. En bestämmelse om längsta lagringstid måste säkerställa att uppgifterna inte får behandlas längre

än nödvändigt. Detta följer av principen om lagringsminimering (jfr 1 kap. 17 § första stycket brottsdatalagen).

I promemorian lämnas ett förslag på att behandling av personuppgifter i form av uppgifter om motorfordon som samlats in genom kamerabevakning som Polismyndigheten eller Säkerhetspolisen bedriver på plats som allmänt används för trafik med motorfordon får ske i sex månader från det att uppgifterna samlades in. Bedömningen är att sex månader får anses vara en tidsrymd som både säkerställer att användning av personuppgifterna får ske tillräckligt länge för att tillgodose ändamålet med kamerabevakningen samtidigt som skyddet för den personliga integriteten värnas. De överväganden som gjorts i detta avseende (se avsnitt 11.2.2) gör sig i vissa avseenden gällande även för vilken längsta tid uppgifter som samlats in genom kamerabevakning och som har gjorts gemensamt tillgängliga ska få behandlas. Den föreslagna bestämmelsen i 3 kap. 2 § första stycket 9 innebär att alla typer av uppgifter från kamerabevakning som sker med stöd av kamerabevakningslagen eller annan författning får göras gemensamt tillgängligt för vissa föreskrivna ändamål. Detta innebär att det är fråga om lagring och bearbetning av en stor mängd personuppgifter av olika karaktär.

En bestämmelse om att material från kamerabevakning som bedrivs med stöd av kamerabevakningslagen eller annan författning får göras gemensamt tillgängligt innebär att både obearbetat och strukturerat material kan göras tillgängligt. Enligt gällande uppfattning får obearbetat material från kamerabevakning vanligen lagras under två månader, om det inte sker för ett specifikt ändamål eller ärende (se avsnitt 11.2.2). Uppfattningen grundar sig i den tidigare gällande kameraövervakningslagen som innehöll en bestämmelse enligt vilken bild- eller ljudmaterial från kamerabevakning av en plats dit allmänheten har tillträde som huvudregel fick bevaras under högst två månader (32 § kameraövervakningslagen [2013:460]). Om materialet däremot användes i någon annan verksamhet än den som bedrevs av den som ansvarade för bevakningen tillämpades dock i stället regleringen i personuppgiftslagen eller annan författning som då gällde för behandling av personuppgifter i den verksamheten. Detta innebar exempelvis att Polismyndigheten inte var begränsad av den föreskrivna lagringstiden, om materialet togs in i en förundersökning. I föregångaren till

kameraövervakningslagen, lagen om allmän kameraövervakning (1998:150), föreskrevs att sådant material endast fick bevaras i, som huvudregel, högst en månad. En något längre bevarandetid ansågs dock med tiden vara motiverad med hänvisning till ett behov av att kunna använda materialet för utredning av brott. Erfarenheter hade visat att många brott upptäcktes först efter att en månad hade gått och att materialet då var raderat. Tiden förlängdes därför till två månader för att bättre möta behoven. (Se prop. 2012/13: 115 s. 123 ff.)

Det faktum att någon tidsgräns för lagring numera inte anges skulle kunna ge en indikation på att det bör vara möjligt att i större utsträckning göra olika bedömningar av tillåten lagringstid och att två månader inte längre är en självklar gräns. Till detta kommer att den under senare tid kraftigt ökade förekomsten av organiserad brottslighet och grova våldsbrott gör att Polismyndighetens och Säkerhetspolisens behov ser annorlunda ut. När det gäller organiserad brottslighet och grova våldsbrott finns det ett ökat behov av att uppgifter får göras gemensamt tillgängliga utan att det finns ett specifikt ärende upplagt. Sådan brottslighet är nämligen mer komplex att bekämpa och föregås ibland av underrättelsearbete med obestämd varaktighet som inte tar sikte på en specifik individ och därmed inte nödvändigtvis utgör ett ärende. För att underrättelseverksamheten ska kunna bedrivas på ett effektivt sätt behöver uppgifter från bl.a. kamerabevakning kunna lagras och bearbetas under en längre tid än några månader. I dag är behovet påtagligt av att kunna kartlägga och analysera uppgifter som inte nödvändigtvis är ärendeanknutna under en längre tid än vad som tidigare ansetts godtagbart. Samtidigt är det av stor vikt att bl.a. principen om lagringsminimering och skyddet för den personliga integriteten beaktas och respekteras.

Att personuppgifter ska kunna behandlas inom ramen för underrättelseverksamhet har slagits fast redan genom att begreppen förebygga, förhindra eller upptäcka brottslig verksamhet räknas upp bland de tillåtna rättsliga grunderna för behandlingen inom ramen för brottsbekämpningen. Att kamerabevakning ska kunna användas som teknik i den verksamheten följer också av att begreppen återfinns i kamerabevakningslagen.

Utredningen om effektivare polisiära åtgärder i gränsnära områden gjorde i betänkandet *Åtgärder i gränsnära områden* (SOU

2021:92) bedömningen att dataskyddsregleringens bestämmelser i regel är tillräckliga för att säkerställa att de brottsbekämpande myndigheterna i tillräcklig utsträckning får tillgång till nödvändig information även inom ramen för underrättelseverksamheten. Därför lämnade utredningen inget förslag om särskilda bestämmelser om bearbetning och lagring av obearbetat videomaterial för kamerabevakning i gränsnära områden. Utredningen framhöll dock att det inte är uteslutet att längre tids behandling skulle kunna bli aktuell i särskilda situationer, eller efter en mer genomgripande reform av regelverket. Utredningens uppdrag bestod av att säkerställa att Polismyndigheten hade förmåga att bekämpa brott i gränsnära områden. Det var alltså fråga om brottslighet inom ett begränsat geografiskt område. I förevarande fall ska föreslås regler som möjliggör för Polismyndigheten och Säkerhetspolisen att använda kamerabevakning i sin verksamhet för att bättre kunna bekämpa organiserad brottslighet och terroristbrottslighet i hela landet. Det är således fråga om mycket allvarlig brottslighet som riktar sig mot liv och hälsa. Brottsligheten i och omkring de gränsnära områdena är i och för sig allvarlig men är i allt väsentligt inte direkt riktad mot människors liv och hälsa på det sätt som sprängningar och skjutningar är.

I sammanhanget kan noteras att lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen, som har sin grund i EU:s PNR-direktiv, innehåller en uttrycklig reglering om insamling och fortsatt behandling i sex månader, och under vissa förutsättningar i fem år, av en omfattande mängd personuppgifter avseende personer som till största del inte är misstänkta för brott. Möjligheten är begränsad till att gälla endast för mycket allvarlig brottslighet, likt sådan som den föreslagna bestämmelsen om att få göra uppgifter från kamerabevakning gemensamt tillgängliga tar sikte på.

Det föreslås att en reglering införs som föreskriver att uppgifter som samlats in genom kamerabevakning med stöd av kamerabevakningslagen eller annan författning som gjorts gemensamt tillgängliga får behandlas i sex månader. Gällande obearbetat material från kamerabevakning innebär detta en utökning av den nu gällande uppfattningen att sådant material får lagras i två månader. Endast särskilt angivna tjänstemän som är i behov av uppgifterna för att upprätthålla allmän ordning och säkerhet eller förebygga, förhindra, upptäcka eller utreda och lagföra ett brott för vilket är föreskrivet

fängelse i tre år eller mer föreslås få tillgång till uppgifterna. Därigenom begränsas spridningen av uppgifterna och risken för otillbörliga intrång i den personliga integriteten minimeras. Utöver detta måste behandlingen ske i överensstämmelse med övrig dataskyddsrättslig reglering. Den föreslagna regleringen är proportionerlig och nödvändig för att tillgodose Polismyndighetens och Säkerhetspolisens behov av att effektivt kunna bekämpa organiserad och grov brottslighet.

Det bör även framhållas att när väl material från kamerabevakning har bearbetats och analyserats för ett mer avgränsat ändamål möjliggör bestämmelserna i 4 kap. polisens brottsdatalag att materialet lagras under längre tid än om det inte finns något sådant ändamål. Den föreslagna bestämmelsen hindrar inte att uppgifter från kameramaterial som hänför sig till ett ärende, exempelvis en förundersökning, kan göras gemensamt tillgängliga med stöd av någon annan bestämmelse i 3 kap. 2 § polisens brottsdatalag och därmed möjliggörs en annan lagringstid enligt 4 kap. samma lag.

11.9 Tydligare reglering av möjligheterna att dela personuppgifter som samlats in från kamerabevakning med Polismyndigheten och Säkerhetspolisen

Förslag: Det ska införas en ny rättslig grund för vidarebehandling av personuppgifter i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Den rättsliga grunden ger privata och offentliga aktörer en möjlighet att – på begäran av Polismyndigheten och Säkerhetspolisen – behandla personuppgifter som samlats in från kamerabevakning för att lämna sådana uppgifter som begärs av respektive myndighet för att utreda ett begånget brott för vilket fängelse är föreskrivet eller för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket fängelse är föreskrivet.

För att få behandla personuppgifter krävs bl.a. att det finns en rättslig grund för behandlingen. För andra aktörer än brottsbekämpande myndigheter finns de rättsliga grunderna reglerade i

artikel 6.1 i dataskyddsförordningen. Behandling av personuppgifter måste vidare alltid ske för ett specifikt ändamål. Möjligheten att vidarebehandla personuppgifter begränsas av den s.k. finalitetsprincipen, vilken kommer till uttryck i artikel 5.1 b i dataskyddsförordningen. Finalitetsprincipen innebär att personuppgifter, efter att de samlats in, inte får behandlas på ett sätt som är oförenligt med det ursprungliga ändamål för vilket de samlats in. Under förutsättning att Polismyndighetens eller Säkerhetspolisens ändamål med behandlingen inte är oförenlig med det ursprungliga insamlingsändamålet kan en aktör alltså lämna ut materialet till myndigheten. För detta krävs dock att materialet inte omfattas av tystnadsplikt.

Av artikel 6.4 i dataskyddsförordningen framgår att om en behandling för andra ändamål än de för vilka personuppgifterna samlades in inte grundar sig på den registrerades samtycke eller på unionsrätten eller medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda de mål som avses i artikel 23.1, ska den personuppgiftsansvarige för att fastställa huruvida behandling för andra ändamål är förenligt med det ändamål för vilket personuppgifterna ursprungligen samlades in göra ett förenlighetstest enligt punkterna a–e i artikel 6.4 när personuppgifterna ska behandlas. Enligt artikel 23.1 d är ett av målen att ”förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten”.

Ett utlämnande som innebär att personuppgifter kommer att behandlas för ett annat ändamål än det ursprungliga insamlingsändamålet kan, enligt artikel 6.4 i dataskyddsförordningen, ske med stöd av bestämmelser i unionsrätten eller nationell rätt. I svensk rätt finns en sådan bestämmelse gällande personuppgifter som samlats in genom kamerabevakning i 32 kap. 3 a § OSL. Enligt bestämmelsen får personuppgifter som inhämtats genom kamerabevakning lämnas ut till bl.a. Polismyndigheten eller Säkerhetspolisen, om uppgiften behövs för att utreda ett begånget brott för vilket fängelse är föreskrivet eller för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket fängelse är föreskrivet. Bestämmelsen bryter sekretessen enligt 32 kap. 3 § OSL som annars gäller för uppgifter om enskilds personliga förhållanden som har

inhämtats genom kamerabevakning. Ett utlämnande som sker i enlighet med 32 kap. 3 a § OSL ska alltid anses förenligt med finalitetsprincipen (se prop. 2012/13:115 s. 111 och HFD 2021 ref. 10).

Polismyndigheten har framfört att det finns en osäkerhet om med vilken laglig rätt aktörer, framför allt privata, har att lämna ut material som innehåller personuppgifter från bevakningskameror till myndigheten. Det kan bl.a. handla om butiker, restauranger och hotell som besitter material från bevakningskameror som kan vara värdefullt för Polismyndigheten eller Säkerhetspolisen att få ta del av för att exempelvis utreda brott. När privata aktörer bedriver kamerabevakning, utan att utföra en uppgift av allmänt intresse, omfattas materialet inte av offentlighets- och sekretesslagens bestämmelser. Regeringen har dock framhållit att obehörighetsrekvisitet i 22 § första stycket kamerabevakningslagen är avsett att tolkas på så sätt att ett uppgiftslämnande av en enskild aktör som motsvarar ett uppgiftslämnande som är tillåtet enligt offentlighets- och sekretesslagen inte är att betrakta som obehörigt. (Se prop. 2017/18:231 s. 157.) Personuppgifter från kamerabevakning som bedrivs av privata aktörer med stöd av kamerabevakningslagen får alltså, på samma sätt som när kamerabevakning bedrivs av offentliga aktörer, vidarebehandlas, om det är förenligt med 32 kap. 3 a § OSL.

Det förekommer även att aktörer bedriver kamerabevakning som faller utanför kamerabevakningslagens tillämpningsområde. Detta gäller bl.a. fysiska personer som bedriver kamerabevakning som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll. Det kan tänkas att Polismyndigheten eller Säkerhetspolisen i vissa fall kan ha intresse av att få tillgång även till material från sådan kamerabevakning. Enligt 5 § första stycket 1 kamerabevakningslagen är lagen inte tillämplig på kamerabevakning av rent privat natur. För behandling av personuppgifter som en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll gäller inte heller dataskyddsförordningens bestämmelser (se artikel 1), varför ett utlämnande i en sådan situation kan ske utan beaktande av nämnda regleringar.

Som framgått ovan behöver en bedömning av förenligheten med artikel 6.4 a–e i dataskyddsförordningen inte göras, om det finns en rättslig grund för vidarebehandlingen i nationell rätt. I Utredningen

om förbättrade möjligheter att utbyta information med brottsbekämpande myndigheters betänkande (SOU 2023:69) föreslås att en ny reglering införs i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning som möjliggör för enskilda att behandla personuppgifter för att lämna sådana uppgifter som begärs av Ekobrottsmyndigheten, Kustbevakningen, Polismyndigheten, Skatteverket, Säkerhetspolisen, Tullverket och Åklagarmyndigheten för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller lagföra brott. Förslaget är under behandling i Regeringskansliet och har i dagsläget inte lett till någon lagändring.

Polismyndigheten har framfört att det finns behov av en uttrycklig bestämmelse som slår fast att enskilda får behandla personuppgifter i syfte att lämna dem till Polismyndigheten eller Säkerhetspolisen när uppgifterna behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller lagföra brott. Som framgått ovan är det redan enligt gällande rätt möjligt för både privata och offentliga aktörer att behandla personuppgifter och lämna ut material från kamerabevakning när det behövs för att utreda ett begånget brott för vilket fängelse är föreskrivet eller för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket fängelse är föreskrivet. Mot bakgrund av den osäkerhet som råder i detta avseende, vilken riskerar att få till följd att Polismyndigheten och Säkerhetspolisen inte får tillgång till all information som myndigheterna lagligen har rätt att få del av, föreslås att det införs en specifik bestämmelse i lagen med kompletterande bestämmelser till EU:s dataskyddsförordning som reglerar detta.

Den föreslagna bestämmelsen utgör en rättslig grund för privata och offentliga aktörer som bedriver verksamhet som faller under dataskyddsförordningens tillämpningsområde att behandla personuppgifter som samlats in från kamerabevakning för att lämna sådana uppgifter som begärs av Polismyndigheten eller Säkerhetspolisen för att utreda ett begånget brott för vilket fängelse är föreskrivet eller för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket fängelse är föreskrivet. Då det i de utpekade situationerna är tillåtet för enskilda att behandla personuppgifter, behöver det inte göras några närmare överväganden om personuppgiftsbehandlingens förenlighet med finalitets-

principen inför ett utlämnande av uppgifter. Den föreslagna utformningen av bestämmelsen möjliggör även personuppgiftsbehandling som sker inför ett utlämnande, t.ex. strukturering eller bearbetning av uppgifter. Bestämmelsen utgör ingen skyldighet att behandla eller lämna ut personuppgifter på en begäran från Polismyndigheten eller Säkerhetspolisen. Den fråntar inte heller den utlämnande aktören från ansvar för att personuppgiftsbehandlingen inte går utöver vad som är nödvändigt för att efterkomma myndighetens begäran, vilket följer av principen om uppgiftsminimering. Om det uppstår tveksamhet i frågan om vilka uppgifter som bör lämnas ut för att tillmötesgå Polismyndighetens eller Säkerhetspolisens begäran bör samråd ske med den begärande myndigheten.

Mot bakgrund av att det redan i gällande rätt finns stöd för vidarebehandling i de situationer som här föreslås bedöms den föreslagna bestämmelsen vara nödvändig och proportionerlig i enlighet med dataskyddsförordningen. Här beaktas även att den behandling av personuppgifter som sker hos Polismyndigheten och Säkerhetspolisen sammantaget är underställd stränga krav enligt brottsdatalagen (2018:1177) och att uppgifterna skyddas av stark sekretess hos de mottagande myndigheterna genom bl.a. bestämmelserna i 18 kap. 1 och 2 §§ och 35 kap. 1 § OSL.

12 Ikraftträdande- och övergångsbestämmelser

12.1 Ikraftträdandebestämmelser

Förslag: Författningsförslaget som rör Polismyndighetens och Säkerhetspolisens möjlighet att få tillstånd att använda system för biometrisk fjärridentifiering i realtid på allmän plats föreslås träda i kraft den dag regeringen bestämmer. Övriga författningsförslag föreslås träda i kraft den 1 januari 2025.

De förslag som lämnas i promemorian om bl.a. utökade möjligheter för Polismyndigheten och Säkerhetspolisen att bedriva kamerabevakning på platser som allmänt används för trafik med motorfordon utan att dessförinnan behöva göra en skriftligt dokumenterad intresseavvägning och behandla vissa personuppgifter som rör motorfordon samt förslagen i övrigt bedöms innebära att Polismyndighetens och Säkerhetspolisens möjligheter att bekämpa brott förbättras, särskilt grov och organiserad brottslighet. Det är därför angeläget att författningsförslagen kan träda i kraft så snart som möjligt.

För att förslaget om att Polismyndigheten och Säkerhetspolisen får ges tillstånd att använda system för biometrisk fjärridentifiering i realtid på allmän plats ska kunna träda i kraft krävs dock att ytterligare bestämmelser införs. Det är fråga om bl.a. föreskrifter om vilken myndighet som ska vara marknadskontrollmyndighet till vilken varje användning av ett system för biometrisk fjärridentifiering i realtid på allmän plats ska anmälas och vilken rättslig eller oberoende administrativ myndighet som ska vara tillståndsgivare för sådana system (se artikel 5 punkterna 4 och 5 AI-

förordningen[26]). Mot denna bakgrund föreslås att regeringen bemyndigas att besluta om när den aktuella bestämmelsen ska träda i kraft. Vad gäller övriga författningsförslag som lämnas föreslås det att dessa ska träda i kraft den 1 januari 2025.

12.2 Övergångsbestämmelser

Bedömning: Det behövs inga övergångsbestämmelser.

De lämnade förslagen gäller personuppgiftsbehandling på olika sätt i form av insamling, användning och lagring. Som huvudregel gäller att redan när personuppgifter samlas in måste ändamålet med behandlingen bestämmas. När personuppgifter väl har samlats in kan nya ändamål för behandlingen i allmänhet inte läggas till efterhand. I vissa fall kan dock behandling av redan insamlade personuppgifter ske för nya ändamål. Detta följer av den allmänna dataskyddsrättsliga principen om ändamålsbegränsning och finalitetsprincipen, som bl.a. kommer till uttryck i artikel 4 och 9 dataskyddsdirektivet och 2 kap. 3 och 4 §§ brottsdatalagen. Fråga om sådant kamerabevakningsmaterial som före ikraftträdandet har samlats in av Polismyndigheten eller Säkerhetspolisen vid kamerabevakning av vägar, gator, torg och annan led eller plats som allmänt används för trafik med motorfordon ska få användas för de ändamål som anges i promemorians förslag till ändring i polisens brottsdatalag efter ikraftträdandet får avgöras genom en bedömning av förenligheten med finalitetsprincipen. Polismyndigheten och Säkerhetspolisen bedriver redan i dagsläget kamerabevakning med ändamålet att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott (jfr 8 § andra stycket 1 kamerabevakningslagen). Det bedöms inte finnas några behov av särskilda övergångsbestämmelser gällande detta författningsförslag. Vad gäller övriga förslag finns inte heller några hinder mot att låta de föreslagna

[26] Europaparlamentets ståndpunkt fastställd vid första behandlingen den 13 mars 2024 inför antagandet av Europaparlamentets och rådets förordning (EU) 2024/… om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (rättsakt om artificiell intelligens).

regleringarna gälla fullt ut från och med ikraftträdandet. Det föreslås därför inga särskilda övergångsbestämmelser.

13 Förslagens konsekvenser

13.1 Inledning

Under arbetets bedrivande har en kontinuerlig bedömning skett av vilka konsekvenser de föreslagna ändringarna och tilläggen förväntas medföra. Nedan redovisas en samlad bedömning av dessa.

13.2 Ekonomiska konsekvenser

13.2.1 Polismyndigheten och Säkerhetspolisen

Det föreslås att en ny reglering införs som ger Polismyndigheten och Säkerhetspolisen möjlighet att bedriva kamerabevakning på vägar, gator, torg och annan led eller plats som allmänt används för trafik med motorfordon. Således kan kamerabevakning komma att bedrivas i större utsträckning än i dag. Förslaget innebär att myndigheterna ges möjlighet att utöka förekomsten av bevakningskameror i den utsträckning som det finns behov av det. De kostnader som kan uppkomma får hanteras inom respektive myndighets anslag.

Eftersom kamerabevakning på vägar, gator, torg och annan led eller plats som allmänt används för trafik föreslås vara befriad från kravet på att en intresseavvägning ska göras innan bevakningen påbörjas kommer den administrativa hanteringen av sådan bevakning att förenklas. Förslaget innebär dock att det kan behöva genomföras en konsekvensbedömning och förhandssamråd med Integritetsskyddsmyndigheten. Mot bakgrund av att ett förhandssamråd kan få betydelse för fler bevakningar än just den som förhandssamrådet gäller kan det ofta bli fråga om en initial kostnad.

Genom förslaget skulle den s.k. SOT-lösningen kunna användas i större utsträckning. I avsnitt 9.3.1 redogörs för denna lösning, som i dagsläget används inom ramen för samverkan mellan Polismyndigheten och andra aktörer som bedriver kamerabevakning. Denna typ av samverkan är dock helt frivillig. Förslaget att Polismyndigheten och Säkerhetspolisen ska få bedriva kamerabevakning på vägar, gator, torg och annan led eller plats som allmänt används för trafik innebär att en sådan samverkan skulle kunna ske med exempelvis Trafikverket, som har olika kameror uppsatta längs de allmänna vägarna. En förutsättning är dock att det finns teknisk kapacitet för SOT-lösningen, vilket Trafikverket har upplyst om att myndigheten i dagsläget saknar.

De lämnade förslagen syftar till att effektivisera Polismyndighetens och Säkerhetspolisens arbete att förebygga, förhindra, upptäcka, utreda och lagföra brott. Genom att förslaget om kamerabevakning på platser som allmänt används för trafik med motorfordon möjliggör användning av automatisk igenkänningsteknik av registreringsskyltar frigörs personella resurser då någon manuell granskning inte behöver ske i samma omfattning och arbetet kan bedrivas mer effektivt. Vidare blir resultatet av granskningen mer träffsäkert. Detta bedöms innebära en kostnadsminskning. Eftersom tekniken i dagsläget redan används, bl.a. i gränsnära områden, bör mjukvara och eventuella nödvändiga riktlinjer och rutiner för automatisk igenkänningsteknik av registreringsskyltar redan finnas, och kunna användas även på de platser som nu blir möjliga för Polismyndigheten och Säkerhetspolisen att kamerabevaka. Den föreslagna regleringen i denna del bedöms därmed inte föranleda några kostnader.

Det lämnas även förslag som syftar till att utöka Polismyndighetens och Säkerhetspolisens möjligheter att ta del av uppgifter, både från andra aktörer och inom den egna myndigheten. Samtliga lämnade förslag i dessa delar innebär bättre möjligheter för Polismyndigheten och Säkerhetspolisen att samla in och ta del av information som kan vara av vikt i exempelvis brottsutredningar, vilket på sikt kan leda till att fler brott klaras upp och fler gärningspersoner lagförs. Att det tydligt framgår i en författning vilken typ av information som kan, och i vissa fall ska, lämnas ut till Polismyndigheten och Säkerhetspolisen innebär att mindre personella resurser behöver läggas på att administrera olika begäran

om att få ta del av information. I den delen bedöms förslagen därmed medföra en potentiell kostnadsminskning.

Genom förslaget att uppgifter från kamerabevakning får göras gemensamt tillgängliga för särskilt angivna tjänstemän som är i behov av uppgifterna för att upprätthålla allmän ordning och säkerhet eller förebygga, förhindra, upptäcka eller utreda och lagföra brott för vilket det är föreskrivet fängelse i tre år eller mer samt att behandlingen får ske i sex månader möjliggörs ett informationsflöde inom Polismyndigheten och Säkerhetspolisen. Detta gäller även för andra brottsbekämpande myndigheter då bestämmelsen innebär att dessa myndigheter kan ges direktåtkomst för uppgifter från kamerabevakning som Polismyndigheten och Säkerhetspolisen bedriver. Att rätt personer har tillgång till rätt information är en viktig förutsättning för en effektiv brottsbekämpning. Förslaget bedöms därmed leda till minskade kostnader.

Ett annat förslag är att enskilda ska få behandla personuppgifter för att lämna ut dessa till Polismyndigheten och Säkerhetspolisen för vissa föreskrivna syften. Förslaget är avsett att undanröja den osäkerhet som finns hos vissa aktörer som mottar en begäran om utlämnande av uppgifter. Förslaget bedöms leda till minskade kostnader hos Polismyndigheten och Säkerhetspolisen då begäran inte bör föranleda lika stor administrativ hantering i form av bl.a. efterföljande frågor. Polismyndigheten och Säkerhetspolisen kan även få del av uppgifterna snabbare. Det kan dock tänkas att det fortfarande kommer finnas ett behov av kontakt mellan den mottagande aktören och den efterfrågande myndigheten bl.a. gällande vilket material som avses. Denna kontakt bedöms rymmas inom ramen för ordinarie arbetsuppgifter och innebär ingen kostnadsökning.

Det föreslås även att Transportstyrelsens uppgiftsskyldighet enligt vägtrafikdataförordningen gällande uppgifter om trängselskatt ska utvidgas till att omfatta uppgifter som Polismyndigheten och Säkerhetspolisen behöver i ett brådskande fall för att förebygga, förhindra, upptäcka eller utreda ett brott för vilket det är föreskrivet fängelse i tre år eller mer, eller ett straffbart försök eller en straffbar förberedelse eller stämpling till eller underlåtenhet att avslöja eller förhindra sådant brott. Uppgiftsskyldigheten föreslås även omfatta uppgifter om infrastrukturavgift. Förslaget innebär att utlämnandet inte behöver föregås av en sekretessprövning eller en bedömning av

om det är förenligt med finalitetsprincipen att uppgifterna lämnas ut. Polismyndigheten och Säkerhetspolisen kan därmed snabbt få del av uppgifter som kan användas för att se vilka platser ett fordon har passerat när det behövs för att bl.a. utreda ett allvarligt brott.

Ett ytterligare förslag som lämnas är att Polismyndigheten och Säkerhetspolisen ska få använda system för biometrisk fjärridentifiering i realtid för vissa snävt angivna syften i enlighet med AI-förordningen. Förslaget innebär inget krav på att sådana system ska användas och medför därför som sådant inte någon kostnad. Genom att Polismyndigheten och Säkerhetspolisen tillåts använda system för biometrisk fjärridentifiering kan stora personella resurser frigöras framför allt i utredningsarbetet. Detta skulle innebära en stor kostnadsminskning. Systemen kan även generera träffsäkra resultat som kan användas som bevis i domstol för att lagföra gärningspersoner. För att den föreslagna bestämmelsen ska kunna genomföras krävs bl.a. att det införs bestämmelser om vilken aktör som ska vara tillståndsgivare. Det torde även krävas bestämmelser om hur systemen får användas. Användning av biometrisk fjärridentifiering i realtid kan således komma till användning först när i AI-förordningen uppställda förutsättningar för dess tillämpning klargjorts. Det finns därför inte skäl att i detta sammanhang närmare ta ställning till de kostnader detta förslag kan medföra.

13.2.2 Integritetsskyddsmyndigheten

Den föreslagna regleringen att Polismyndigheten och Säkerhetspolisen får bedriva kamerabevakning på vägar, gator, torg och annan led eller plats som allmänt används för trafik med motorfordon utan att en intresseavvägning först görs kan innebära att Integritetsskyddsmyndigheten kommer behöva utöva tillsyn i viss ökad utsträckning. Det kan även tänkas att det behöver ske fler samråd, eftersom kamerabevakning ofta innebär en omfattande insamling av personuppgifter. Detta är dock helt beroende av i vilken omfattning och på vilket sätt Polismyndigheten och Säkerhetspolisen kommer att bedriva kamerabevakning på aktuella platser. Den eventuella kostnadsökningen för ett utökat samråd får anses rymmas inom Integritetsskyddsmyndigheten befintliga anslag.

13.2.3 Transportstyrelsen

Den föreslagna utvidgningen av Transportstyrelsens uppgiftsskyldighet enligt vägtrafikdataförordningen gällande uppgifter om trängselskatt och infrastrukturavgift innebär att myndigheten i fler situationer än tidigare är skyldig att utan dröjsmål lämna ut uppgifter som Polismyndigheten eller Säkerhetspolisen begär att få ta del av. Eftersom en uppgiftsskyldighet innebär att ett utlämnade inte behöver föregås av en sekretessprövning eller en bedömning om förenligheten med finalitetsprincipen blir hanteringen av en sådan begäran enklare. De ökade personella kostnader som utökningen av uppgiftsskyldigheten kan tänkas innebära anses marginella och bedöms rymmas inom Transportstyrelsens befintliga anslag.

13.2.4 Trafikverket

Som nämnts ovan innebär det föreslagna tillägget i kamerabevakningslagen att samverkan genom en SOT-lösning skulle kunna bli aktuell för Trafikverkets kameror på allmänna vägar. Eftersom Trafikverket har upplyst om att en sådan teknisk lösning i dagsläget saknas skulle detta innebära en kostnad i form av att bl.a. en ny mjukvara behöver tas fram. En sådan samverkan är dock helt frivillig. De lämnade förslagen påverkar inte Trafikverkets ekonomi.

13.2.5 Domstols- och åklagarväsendena

De förslag som lämnas bör leda till att fler grova brott klaras upp, vilket bl.a. får till följd att fler åtal kommer att väckas vid domstol. Det är mycket svårt att uppskatta om och i så fall vilken kostnadsökning detta innebär för de allmänna domstolarna och åklagarväsendet. Det kan även tänkas att fler tillsynsbeslut om kamerabevakning kan förekomma i allmän förvaltningsdomstol. Eventuella kostnadsökningar bedöms dock rymmas inom domstolarnas och åklagarväsendets befintliga anslag.

13.2.6 Enskilda aktörer

För att undanröja den osäkerhet som föreligger hos aktörer som mottar en begäran från Polismyndigheten eller Säkerhetspolisen om utlämnande av material från kamerabevakning lämnas ett förslag på en reglerad möjlighet för enskilda aktörer, privata och offentliga, att behandla personuppgifter som samlats in genom kamerabevakning för att lämna uppgifterna till Polismyndigheten och Säkerhetspolisen när det behövs för att utreda ett begånget brott för vilket fängelse är föreskrivet eller för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket fängelse är föreskrivet. Genom regleringen tydliggörs att enskilda aktörer får behandla personuppgifter för föreskrivna syften. Detta bedöms innebära färre tidskrävande bedömningar för enskilda aktörer vid en begäran från Polismyndigheten eller Säkerhetspolisen om att få ta del av material från kamerabevakning.

Samtliga förslag förväntas förbättra förutsättningarna för att bekämpa olika typer av brottslighet, vilket bl.a. får positiva ekonomiska konsekvenser för enskilda aktörer och samhället i stort.

13.3 Konsekvenser för den personliga integriteten och andra grundläggande fri- och rättigheter

De föreslagna ändringarna och tilläggen innebär utökade möjligheter för Polismyndigheten och Säkerhetspolisen att behandla personuppgifter. Förslagen möjliggör även för andra brottsbekämpande myndigheter att ta del av uppgifter som samlats in genom kamerabevakning som Polismyndigheten och Säkerhetspolisen bedriver. Hantering av personuppgifter måste alltid vara förenlig med regleringen om dataskydd. Bestämmelser om personuppgiftshantering måste vidare alltid beakta skyddet för den personliga integriteten och rätten till privat- och familjeliv. Vissa intrång i de senare nämnda fri- och rättigheterna får ibland tålas för att exempelvis brottsbekämpande myndigheter ska kunna bekämpa brott på ett effektivt sätt. En bestämmelse som innebär ett intrång i den personliga integriteten och rätten till privat- och familjeliv måste dock alltid vara proportionerlig och nödvändig i förhållande till bestämmelsens ändamål. Proportionalitet och nödvändighet är något som förändras i takt med att samhällsutvecklingen förändras.

Det kan t.ex. handla om att samhället måste reagera på ett adekvat sätt på en allvarlig brottslighetsutveckling som på sikt riskerar att ha allvarliga konsekvenser för enskildas fri- och rättigheter.

Det är generellt svårt att med säkerhet bedöma konsekvenserna för den personliga integriteten och skyddet för rätten till privat- och familjeliv med anledning av förslaget om att Polismyndigheten och Säkerhetspolisen får bedriva kamerabevakning på vägar, gator, torg och annan led eller plats som allmänt används för trafik med motorfordon. Detta beror på den inneboende svårigheten att mäta effekten av kamerabevakning samt att det även får betydelse hur många kameror Polismyndigheten och Säkerhetspolisen väljer att sätta upp, på vilka vägar de sätts upp och hur bevakningen sker. Det står dock klart att den föreslagna regleringen innebär att kamerabevakning kan komma att bedrivas i större utsträckning än i dag. Detta innebär att enskilda kommer att bevakas i större omfattning, vilket kan utgöra en ökad risk för intrång i den enskildes personliga integritet. Denna risk begränsas genom att det föreslås en bestämmelse om vilka typer av personuppgifter som får behandlas samt för vilka ändamål och hur länge de uppgifter som samlas in genom kamerabevakning på angivna platser får användas. Utöver den föreslagna begränsningen gäller även övriga dataskyddsrättsliga regler, vilka ger ett starkt skydd mot otillbörliga intrång i den personliga integriteten. Det kan förutsättas att kameror kommer att sättas upp endast där det finns stora behov av det. Vidare har kamerabevakning nödvändigtvis inte bara negativa följder för den personliga integriteten. Om kamerabevakning medför ökad trygghet och minskad brottslighet kan det anses förstärka skyddet för den personliga tryggheten och integriteten (jfr prop. 2018/17:147 s. 58). Det föreslås inte att upplysnings- och skyltningskravet ska tas bort. Det kommer därmed vara tydligt var kamerabevakning bedrivs, vilket möjliggör för den enskilde att undvika att bli kamerabevakad.

Ett annat förslag som lämnas är att personuppgifter från kamerabevakning ska få göras gemensamt tillgängliga inom Polismyndigheten och Säkerhetspolisen. Förslaget innebär att andra brottsbekämpande myndigheter får ges direktåtkomst till uppgifterna. Det föreslås även att Transportstyrelsen ska vara skyldig att lämna ut fler uppgifter till Polismyndigheten och Säkerhetspolisen. När personuppgifter blir tillgängliga för fler personer ökar riskerna för otillbörliga intrång i den personliga

integriteten. Genom att det föreslås att tillgången till material från kamerabevakning ska begränsas till särskilt angivna tjänstemän som är i behov av uppgifterna för att upprätthålla allmän ordning och säkerhet eller förebygga, förhindra, upptäcka eller utreda och lagföra brott för vilket det är föreskrivet fängelse i tre år eller mer minimeras risken för ett obefogat integritetsintrång. Det tydliggörs även att material från kamerabevakning endast får delas inom myndigheten i den mån det är nödvändigt för föreskrivna syften. Till detta kommer att Polismyndigheten har fört fram att det kommer att innebära en mycket påtaglig effektivitetsvinst i den brottsbekämpande verksamheten att myndigheterna i större utsträckning få göra de aktuella uppgifterna gemensamt tillgängliga. Polismyndighetens och Säkerhetspolisens möjligheter att bekämpa grova brott kommer därmed förbättras. Den effektivisering av det brottsbekämpande arbetet som kan förutses innebär alltså i sig i viss mån att personer som riskerar att utsättas för brott känner en ökad trygghet. Det är vidare frivilligt att göra uppgifterna direkt åtkomliga för andra brottsbekämpande myndigheter. Vid direktåtkomst har samma begränsning om tillgång till personuppgifter ansetts gälla hos den mottagande myndighet (prop. 2009/10:85 s. 177). Uppgifterna som Transportstyrelsens utvidgade uppgiftsskyldighet omfattar är främst uppgifter om fordon och passager av olika kontrollpunkter. Sådana uppgifter får anses utgöra mindre känsliga personuppgifter.

Det föreslås även att Polismyndigheten och Säkerhetspolisen ska få använda system för biometrisk fjärridentifiering i realtid för vissa snävt angivna syften i enlighet med den kommande AI-förordningen. Användning av sådana system innebär ett potentiellt stort ingrepp i den personliga integriteten då de möjliggör bevakning av ett stort antal människor och innebär behandling av känsliga uppgifter i form av biometriska personuppgifter. Det är därför viktigt att användning av sådana system endast sker när det är absolut nödvändigt och proportionerligt. Genom att den föreslagna regleringen bl.a. slår fast att systemen får användas endast för vissa brott för vilka det är föreskrivet minst fyra års fängelse görs det tydligt att det bara är vid allvarlig brottslighet som biometrisk fjärridentifiering i realtid kan komma i fråga för att lokalisera eller identifiera en misstänkt gärningsperson. Enligt AI-förordningen krävs som huvudregel att en rättslig myndighet eller en oberoende administrativ myndighet ger tillstånd till sådan användning. För att

den föreslagna bestämmelsen ska kunna genomföras krävs att det införs bestämmelser om vilken aktör som ska vara tillståndsgivare. Det torde även krävas ytterligare bestämmelser om hur systemen och utdata från dessa får användas. Utöver begränsningen att systemen enbart får användas för föreskrivna syften för brottsbekämpningsändamål när det är absolut nödvändigt utgör nämnda kompletterande bestämmelser ett ytterligare skydd för den personliga integriteten.

De föreslagna tilläggen och ändringarna har noga vägts mot det intrång i den personliga integriteten som förslagen innebär. Vid denna intresseavvägning har särskilt beaktats att det finns ett påtagligt behov av att komma till rätta med en ökad gängkriminalitet och negativ brottsutveckling. Detta behov är så pass stort att det innebär att de eventuella inskränkningar i enskildas fri- och rättigheter som lämnade förslag kan medföra är nödvändiga och proportionerliga. Kamerabevakning och informationsutbyte kan många gånger utgöra viktiga verktyg i Polismyndighetens och Säkerhetspolisens arbete att utreda och förhindra brott samt lagföra personer som har begått brott.

Ett eventuellt ökat intrång i den personliga integriteten för vissa människor innebär samtidigt en ökad trygghet för andra människor.

13.4 Konsekvenser för det brottsbekämpande arbetet

Precis som med bedömningen av konsekvenserna för den personliga integriteten är det generellt svårt att med säkerhet avgöra vilken betydelse för den brottsutredande verksamheten och det brottsförebyggande arbetet den föreslagna regleringen om kamerabevakning på vägar, gator, torg och annan led eller plats som allmänt används för trafik med motorfordonkan tänkas få. Detta med anledning av den inneliggande svårigheten att mäta effekten av kamerabevakning samt då detta även avgörs av hur många kameror som Polismyndigheten och Säkerhetspolisen sätter upp och på vilka platser de sätts upp. Kamerabevakning och informationsutbyte fyller dock en viktig funktion och utgör väsentliga verktyg i brottsbekämpningen. Det har bl.a. ett stort värde för myndigheternas underrättelseverksamhet samt vid utredningar av brott och som bevis i domstol. Genom att Polismyndigheten och Säkerhetspolisen

utifrån de föreslagna ändringarna och tilläggen kan kamerabevaka på fler platser, göra uppgifter från kamerabevakning gemensamt tillgängliga och behandla dessa under längre tid, få del av information från andra aktörer och för vissa syften få använda sig av biometrisk fjärridentifiering i realtid kan arbetet med att bekämpa, utreda och lagföra brott förbättras och effektiveras. Detta bedöms leda till att utredningstider kortas samt att fler brott kan klaras upp och fler gärningspersoner lagföras. Förslagen möjliggör bl.a. att Polismyndigheten och Säkerhetspolisen kan få information om hur ett fordon färdas, vilket är viktig information då olagliga transporter av människor och varor ofta sker på vägar. Genom att förutsättningarna för att bekämpa och lagföra brott förbättras kan förslagen på sikt bidra till att tryggheten i samhället ökar, att brottsligheten minskar och att fler brott förhindras.

14 Författningskommentar

14.1 Förslaget till lag om ändring i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

2 kap. Grundläggande bestämmelser om behandling av personuppgifter

Möjligheter för enskilda att lämna uppgifter som samlats in från kamerabevakning till Polismyndigheten och Säkerhetspolisen

5 § *Enskilda får behandla personuppgifter som samlats in från kamerabevakning för att lämna sådana uppgifter som begärs av Polismyndigheten eller Säkerhetspolisen för att utreda ett begånget brott för vilket fängelse är föreskrivet eller för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket fängelse är föreskrivet.*

Paragrafen, som är ny, innehåller en rättslig grund för privata och offentliga aktörer som bedriver verksamhet som faller under dataskyddsförordningens tillämpningsområde att behandla personuppgifter som samlats in genom kamerabevakning för att lämna sådana uppgifter som begärs av Polismyndigheten eller Säkerhetspolisen för att utreda ett begånget brott för vilket fängelse är föreskrivet eller för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket fängelse är föreskrivet.

Bestämmelsen utnyttjar det utrymme som ges i artikel 6.4 i dataskyddsförordningen att införa regler i nationell rätt som tillåter

behandling av personuppgifter för nya ändamål, förutsatt att en sådan bestämmelse utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle som syftar till att skydda vissa mål som anges i artikel 23.1 i dataskyddsförordningen. Bland dessa återfinns den nationella och den allmänna säkerheten liksom förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten.

Bestämmelsen möjliggör att personuppgifter får behandlas för de ändamål som föreskrivs, oavsett om det är förenligt med det ursprungliga insamlingsändamålet eller inte. Detta medför att den utlämnande aktören inte behöver bedöma om behandlingen av personuppgifter är förenlig med den s.k. finalitetsprincipen i artikel 5.1 b i dataskyddsförordningen.

Behandling av personuppgifter enligt bestämmelsen är bara tillåten om den sker i syfte att lämna ut uppgifter till Polismyndigheten eller Säkerhetspolisen. Det ska vara fråga om uppgifter som behövs för att utreda ett begånget brott för vilket fängelse är föreskrivet eller för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket fängelse är föreskrivet. Bestämmelsen ger därmed inte enskilda rätt att behandla personuppgifter för utlämnande till annan verksamhet som dessa myndigheter kan bedriva t.ex. för att verkställa straffrättsliga påföljder, upprätthålla allmän ordning och säkerhet eller sådan kontrollverksamhet som Polismyndigheten i vissa fall bedriver.

Bestämmelsen ska inte tolkas på så sätt att det är otillåtet att lämna ut uppgifter till Polismyndigheten och Säkerhetspolisen i andra situationer än de som uttryckligen omfattas av bestämmelsen, eller att det skulle vara otillåtet att lämna ut uppgifter till andra brottsbekämpande myndigheter. Möjligheten att behandla personuppgifter i en sådan situation får avgöras av annan tillämplig dataskyddsrättslig reglering.

Bestämmelsen möjliggör även personuppgiftsbehandling som sker inför ett utlämnande, t.ex. strukturering eller bearbetning av uppgifter. Den fråntar dock inte den utlämnande aktörens ansvar för att personuppgiftsbehandlingen inte går utöver vad som är nödvändigt för att efterkomma myndighetens begäran, vilket följer av principen om uppgiftsminimering. Om det uppstår tveksamhet i

frågan om vilka uppgifter som bör lämnas ut för att tillmötesgå Polismyndighetens eller Säkerhetspolisens begäran bör samråd ske med den begärande myndigheten. Bestämmelsen medför inte någon skyldighet att lämna ut eller på annat sätt behandla personuppgifter.

Övervägandena finns i avsnitt 11.9.

14.2 Förslaget till lag om ändring i kamerabevakningslagen (2018:1200)

14 c § Bestämmelserna i 14 a och 14 b §§ gäller inte vid

1. kamerabevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning,
2. kamerabevakning som Kustbevakningen, Polismyndigheten, Säkerhetspolisen eller Tullverket bedriver i fall som avses i 9 § 2 och 6–10,
3. kamerabevakning som Kustbevakningen, Polismyndigheten, Säkerhetspolisen eller Tullverket bedriver i gränsnära områden som avses i 2 § lagen (2023:474) om polisiära befogenheter i gränsnära områden, eller av tillfartsvägar till sådana gränsnära områden som avses i 2 § 3 eller 4 samma lag, om bevakningen bedrivs inom 20 kilometer från området *och*
4. *annan kamerabevakning som Polismyndigheten eller Säkerhetspolisen bedriver av väg, gata, torg och annan led eller plats som allmänt används för trafik med motorfordon.*

Paragrafen utgör ett undantag från bestämmelserna i 14 a och 14 b §§ som reglerar förutsättningarna för bl.a. Polismyndigheten och Säkerhetspolisen att bedriva kamerabevakning. Innebörden av paragrafen är att Polismyndigheten och Säkerhetspolisen i vissa fall kan bedriva kamerabevakning utan att först behöva göra en bedömning av om intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad och utan att dokumentera denna bedömning.

I paragrafen görs ett tillägg i form av en ny *fjärde punkt* i vilken det föreskrivs att bestämmelserna i 14 a och 14 b §§ kamera-

bevakningslagen inte ska gälla för annan kamerabevakning än sådan som omfattas av punkterna 1–3 och som Polismyndigheten och Säkerhetspolisen bedriver av väg, gata, torg och annan led eller plats som allmänt används för trafik med motorfordon. Begreppet väg har samma innebörd här som i 2 § förordningen (2001:651) om vägtrafikdefinitioner.

De platser som omfattas av undantaget ska allmänt användas för trafik med motorfordon. Därmed omfattas i allt väsentligt inte enskilda vägar av undantaget.

Den nya punkten gäller endast när Polismyndigheten och Säkerhetspolisen bedriver kamerabevakning av väg, gata, torg och annan led eller plats som allmänt används för trafik med motorfordon. Bestämmelsen är således inte tillämplig på Kustbevakningens och Tullverkets kamerabevakning av väg, gata, torg och annan led eller plats som allmänt används för trafik med motorfordon.

Övervägande finns i avsnitt 11.2.1.

14.3 Förslaget till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område

2 kap. Grundläggande bestämmelser om behandling av personuppgifter

1 a § Personuppgifter som rör motorfordon och som har samlats in genom kamerabevakning som bedrivs med stöd av 14 c § 4 kamerabevakningslagen (2018:1200) får behandlas av Polismyndigheten och Säkerhetspolisen endast om syftet med behandlingen är att förebygga, förhindra, upptäcka, utreda eller lagföra brott för vilket det är föreskrivet fängelse i tre år eller mer. Sådan behandling får alltid ske i sex månader efter det att uppgifterna samlades in.

Första stycket gäller inte för personuppgifter i form av bilder av enskilda.

Paragrafen, som är ny, reglerar för vilket ändamål och hur länge Polismyndigheten och Säkerhetspolisen får använda person-

uppgifter som samlats in med stöd av bestämmelsen 14 c § 4 kamerabevakningslagen. Den reglerar även vilka personuppgifter som får användas. Överväganden finns i avsnitt 11.2.2.

Bestämmelsen kompletterar brottsdatalagen (2018:1177) och de föreskrifter som har meddelats i anslutning till den lagen, liksom andra föreskrifter som genomför dataskyddsdirektivet (se 1 kap. 5 § brottsdatalagen).

Bestämmelsen i *första stycket* föreskriver att de personuppgifter som Polismyndigheten och Säkerhetspolisen får använda är personuppgifter som rör motorfordon. Uppgifterna måste ha samlats in genom kamerabevakning av väg, gata, torg och annan led eller plats som allmänt används för trafik med motorfordon med stöd av bestämmelsen 14 c § 4 kamerabevakningslagen. De uppgifter som kan bli aktuella att använda är t.ex. ett motorfordons registreringsnummer, registreringsland och modell. Det kan också handla om uppgifter om plats och tidpunkt för ett motorfordons passage av en kamera. Med motorfordon avses detsamma som i 2 § lagen (2001:559) om vägtrafikdefinitioner. En förutsättning för bestämmelsens tillämplighet är att uppgifterna utgör personuppgifter. Begreppet personuppgifter är avsett att ha samma innebörd som i 1 kap. 6 § brottsdatalagen (jfr prop. 2022/23:109 s. 52).

Bestämmelsen begränsar för vilket ändamål personuppgifter som rör motorfordon som samlats in från kamerabevakning som bedrivs av väg, gata, torg och annan led eller plats som allmänt används för trafik med motorfordon stöd av bestämmelsen i kamerabevakningslagen får användas. För att Polismyndigheten och Säkerhetspolisen ska få använda uppgifterna måste syftet med användningen vara att förebygga, förhindra, upptäcka, utreda eller lagföra brott för vilket det är föreskrivet fängelse i tre år eller mer. Bestämmelsen är teknikneutral och inrymmer användning av personuppgifter som rör motorfordon som har samlats in med bl.a. ANPR-teknik.

Om användningen av personuppgifter som rör motorfordon sker för andra ändamål än att förebygga, förhindra, upptäcka, utreda eller lagföra brott för vilket det är föreskrivet fängelse i tre år eller mer, eller om uppgifter om motorfordon som samlats in för detta ändamål används för nya ändamål efter insamlingen, måste användningen ha stöd i andra tillämpliga bestämmelser i det dataskyddsrättsliga regelverket. Likaså måste uppgifterna ha samlats

in genom kamerabevakning, vilket innebär att de ska framgå av material från kamerabevakningen. Bestämmelsen är därmed inte tillämplig på uppgifter som kommer fram t.ex. genom att material från kamerabevakning jämförs med olika register. Om det vid en sådan jämförelse framkommer uppgift om t.ex. vem som är ägare till ett motorfordon får den uppgiften alltså användas endast med stöd av annan tillämplig dataskyddsreglering.

Personuppgifter om motorfordon som samlats in på väg, gata, torg och annan led eller plats som allmänt används för trafik med motorfordon med stöd av bestämmelsen 14 c § 4 kamerabevakningslagen får alltid användas av Polismyndigheten och Säkerhetspolisen för de i förevarande bestämmelse föreskrivna ändamålen i sex månader från det att de samlades in. I vissa fall kan det finnas stöd i 4 kap. polisens brottsdatalag för att använda personuppgifter som rör motorfordon under längre tid.

Enligt paragrafens *andra stycke* gäller första stycket inte för personuppgifter i form av bilder av enskilda, det vill säga sådana bilder av enskilda som direkt eller indirekt kan identifiera en person. För användning av sådana bilder måste stöd i stället finnas i annan tillämplig dataskyddsreglering.

Bestämmelsen är begränsad till att tillämpas på Polismyndighetens och Säkerhetspolisens användning av personuppgifter om motorfordon som samlats in med stöd av den föreslagna bestämmelsen 14 c § 4 kamerabevakningslagen. Bestämmelsen är således inte tillämplig på någon annan brottsbekämpande myndighets användning av sådana personuppgifter.

2 § Förutsättningarna för att behandla personuppgifter som behandlas med stöd av 1 *eller 1 a §* för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:1177).

Tillägget i paragrafen är en följd av att det införs en ny rättslig grund i 1 a § för användning av personuppgifter om motorfordon som samlats in genom kamerabevakning av väg, gata, torg och annan led eller plats som allmänt används för trafik med motorfordon med stöd av bestämmelsen 14 c § 4 kamerabevakningslagen.

4 a § *Polismyndigheten och Säkerhetspolisen får ges tillstånd att använda system för biometrisk fjärridentifiering i realtid på allmän*

plats under de förutsättningar och för de syften som anges i artikel 5.1 h i EU:s förordning om artificiell intelligens[27].

Paragrafen, som är ny, reglerar för vilka syften och under vilka förutsättningar Polismyndigheten och Säkerhetspolisen får beviljas tillstånd att använda system för biometrisk fjärridentifiering i realtid för brottsbekämpningsändamål. Precis som med övrig behandling av biometriska personuppgifter måste användningen vara absolut nödvändig för att tillstånd ska få ges.

Bestämmelsen är tillämplig på Polismyndighetens verksamhet att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, eller upprätthålla allmän ordning och säkerhet samt på Säkerhetspolisens verksamhet gällande frågor som inte rör nationell säkerhet i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott (jfr 1 kap. 1 § polisens brottsdatalag och artikel 3.45 och 3.46 i EU:s förordning om AI).

Biometrisk fjärridentifiering i realtid är ett system för biometrisk fjärridentifiering där infångning av biometriska uppgifter, jämförelse och identifiering sker utan betydande dröjsmål och omfattar inte bara omedelbar identifiering utan även begränsade korta fördröjningar för att undvika kringgående (artikel 3.42 AI-förordningen).

Begreppet allmän plats har här samma innebörd som i brottsbalken, det vill säga alla platser som allmänheten har tillträde till.

Tillstånd får bl.a. ges för att möjliggöra eftersökning av försvunna personer och offer för exempelvis barnpornografibrott och sådana brott som regleras i 6 kap. BrB och för att förhindra ett överhängande hot mot fysiska personers liv eller fysiska säkerhet eller en sådan handling som kan utgöra terroristbrott enligt 4 § terroristbrottslagen (2022:666). Även lokalisering eller identifiering av en person som misstänks ha begått ett brott, i syfte att genomföra en brottsutredning, lagföring eller ett verkställande av en straff-

[27] Europaparlamentets ståndpunkt fastställd vid första behandlingen den 13 mars 2024 inför antagandet av Europaparlamentets och rådets förordning (EU) 2024/… om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (rättsakt om artificiell intelligens).

rättslig påföljd för vissa utpekade allvarliga brott omfattas av bestämmelsen.

Övervägandena finns i avsnitt 11.4.

3 kap. Gemensamt tillgängliga uppgifter

2 § Följande personuppgifter får göras gemensamt tillgängliga:

1. Uppgifter som kan antas ha samband med misstänkt brottslig verksamhet, om den misstänkta verksamheten
   a) innefattar brott för vilket det är föreskrivet fängelse i ett år eller mer, eller
   b) sker systematiskt.
2. Uppgifter som behövs för övervakningen av en person som
   a) kan antas komma att begå brott för vilket det är föreskrivet fängelse i två år eller mer, och
   b) är allvarligt kriminellt belastad eller kan antas utgöra ett hot mot andras personliga säkerhet.
3. Uppgifter som förekommer i ett ärende om utredning av eller lagföring för brott.
4. Uppgifter som förekommer i ett ärende om uppbörd.
5. Uppgifter som förekommer i ett ärende om kontaktförbud eller om personskydd.
6. Uppgifter som har rapporterats till Polismyndighetens ledningscentraler.
7. Uppgifter som behandlas i syfte att upprätthålla allmän ordning och säkerhet.
8. Uppgifter som behandlas i syfte att fullgöra internationella åtaganden, om det krävs för att den aktuella förpliktelsen ska kunna fullgöras.
9. *Uppgifter som har samlats in genom kamerabevakning med stöd av kamerabevakningslagen (2018:1200) eller annan författning.*

Dna-profiler får inte göras gemensamt tillgängliga. Att sådana uppgifter får behandlas i särskilda register följer av 5 kap.

Tillgången till uppgifter som görs gemensamt tillgängliga med stöd av första stycket 2 ska begränsas till särskilt angivna tjänstemän som har till uppgift att arbeta med övervakningen. Information om att en person är föremål för övervakning får dock göras tillgänglig för andra.

Tillgången till uppgifter som görs gemensamt tillgängliga med stöd av första stycket 9 ska begränsas till särskilt angivna tjänstemän som är i behov av uppgifterna för att upprätthålla allmän ordning och säkerhet eller förebygga, förhindra, upptäcka eller utreda och lagföra brott för vilket det är föreskrivet fängelse i tre år eller mer.

Paragrafen anger vilka personuppgifter som får göras gemensamt tillgängliga. Med gemensamt tillgängliga uppgifter avses inte sådana uppgifter som endast ett fåtal personer har rätt att ta del av (3 kap. 1 § första stycket polisens brottsdatalag). En tumregel för hur många personer som avses med ett fåtal är ett tiotal (prop. 2009/10:85 s. 128 f.).

I paragrafen görs ett tillägg i första stycket i form av en ny *nionde punkt* som möjliggör att uppgifter som samlats in genom kamerabevakning med stöd av kamerabevakningslagen (2018:1200) eller annan författning får göras gemensamt tillgängliga.

I paragrafen görs även ett tillägg i form av ett nytt *fjärde stycke* som begränsar tillgången till uppgifter enligt första stycket 9. Endast särskilt angivna tjänstemän som är i behov av uppgifterna för att upprätthålla allmän ordning och säkerhet eller förebygga, förhindra, upptäcka eller utreda och lagföra brott för vilket det är föreskrivet fängelse i tre år eller mer får ges tillgång till sådana uppgifter. Begränsningen minimerar riskerna för otillbörliga intrång i den personliga integriteten.

Genom att uppgifter från kamerabevakning görs gemensamt tillgängliga kan Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket medges direktåtkomst till uppgifterna för ett syfte som anges i 1 kap. 2 § brottsdatalagen. Detta framgår av 3 kap. 7 § polisens brottsdatalag. Direktåtkomst får endast medges till uppgifter som kan lämnas ut utan hinder av sekretess. Uppgift om en enskilds personliga förhållanden som samlats in genom kamera-

bevakning som avses i kamerabevakningslagen kan lämnas ut till vissa brottsbekämpande myndigheter, om uppgiften behövs för att utreda ett begånget brott för vilket fängelse är föreskrivet eller för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket fängelse är föreskrivet med stöd av 32 kap. 3 a § OSL. Vid direktåtkomst har samma begränsning om tillgång till personuppgifter ansetts gälla hos den mottagande myndighet (prop. 2009/10:85 s. 177).

Övervägandena finns i avsnitt 11.7.

4 kap. Längsta tid som personuppgifter får behandlas

6 § Personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § första stycket 1, 2 eller *5–9* får som längst behandlas under den tid som anges i *7–11 a §§*.

Bestämmelsen i 2 kap. 17 § andra stycket brottsdatalagen (2018:1177) gäller inte vid tillämpningen av *7–11 a §§*.

Paragrafen är ändrad med hänsyn till att det införs en ny punkt i 3 kap. 2 § första stycket som reglerar att personuppgifter som samlats in genom kamerabevakning med stöd av kamerabevakningslagen (2018:1200) eller annan författning får göras gemensamt tillgängliga samt då det införs en ny bestämmelse i 4 kap. 11 a § som reglerar vilken längsta tid sådana personuppgifter får behandlas.

11 a § *Personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § första stycket 9 får inte behandlas längre än sex månader efter det att de samlades in.*

Paragrafen, som är ny, reglerar vilken längsta tid personuppgifter som samlats in genom kamerabevakning med stöd av kamerabevakningslagen (2018:1200) eller annan författning och som gjorts gemensamt tillgängliga får behandlas. Bestämmelsen möjliggör att både obearbetat och strukturerat material från kamerabevakning får bearbetas och lagras i sex månader. Den föreslagna bestämmelsen hindrar inte att uppgifter från kameramaterial som hänför sig till ett ärende, exempelvis en förundersökning, kan göras gemensamt tillgängliga med stöd av någon annan bestämmelse i 3 kap. 2 §

polisens brottsdatalag. Därmed möjliggörs en annan lagringstid enligt 4 kap. samma lag.

Övervägandena finns i avsnitt 11.8.

12 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att vissa kategorier av personuppgifter får fortsätta att behandlas för ändamål inom denna lags tillämpningsområde under längre tid än vad som anges i 3, 4 eller *7–11 a §*.

Paragrafen är ändrad med hänsyn till att det införs en ny bestämmelse i 4 kap. 11 a § som reglerar vilken längsta tid personuppgifter som gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § första stycket 9 får behandlas.

13 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att personuppgifter får behandlas för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål under längre tid än vad som anges i 2 § första stycket eller *7–11 a §* och
2. begränsning av behandlingen av personuppgifter för ändamål inom denna lags tillämpningsområde vid digital arkivering.

Paragrafen är ändrad med hänsyn till att det införs en ny bestämmelse i 4 kap. 11 a § som reglerar vilken längsta tid personuppgifter som gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § första stycket 9 får behandlas.

Regeringskansliet

Bilaga

2023-11-29

Justitiedepartementet
Enheten för lagstiftning om allmän ordning och säkerhet

Uppdrag att förbättra polisens möjlighet till kamerabevakning

1. Uppdraget i korthet

En utredare ges i uppdrag att förbättra förutsättningarna för Polismyndigheten och Säkerhetspolisen att använda kamerabevakning i sin verksamhet.

Utredaren ska bl.a. lämna författningsförslag som gör att polisen i större utsträckning och på ett verkningsfullt sätt kan

- använda teknik som innebär kamerabevakning med automatisk ansiktsigenkänning och igenkänning av registreringsnummer, och
- få ta del av bevakningsmaterial från annans kamerabevakning.

Uppdraget ska redovisas senast den 29 maj 2024.

2. Bakgrund och behovet av en utredning

Organiserad brottslighet och terroristbrottslighet utgör allvarliga hot mot enskilda, men också mot samhället i stort. Brottsutvecklingen med skjutningar och sprängningar är exceptionell och det föreligger en förhöjd hotnivå i Sverige. Det finns därför ett mycket angeläget behov av att säkerställa att de brottsbekämpande myndigheterna får utökad tillgång till effektiva, resurssparande och kraftfulla verktyg. Kamerabevakning är ett viktigt inslag i det polisiära arbetet. Det kan användas i såväl brotts-förebyggande arbete som brottsutredande arbete. Med hjälp av kamerabevakning kan polisen exempelvis hitta, identifiera och följa kriminella aktörer. Kamerautrustning i olika former finns i dag hos t.ex. myndigheter, kommuner och regioner samt hos privata aktörer.

Förutsättningarna för kamerabevakning styrs av kamerabevakningslagen (2018:1200) och regelverket för behandling av personuppgifter, bl.a. brottsdatalagen (2018:1177) och lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter (Säkerhetspolisens datalag). Vid kamerabevakning behöver det ske en intresseavvägning mellan behovet av bevakning och risken för intrång i den personliga integriteten.

I svensk rätt finns ingen definition av begreppet integritet. En kränkning av den personliga integriteten kan beskrivas som ett intrång i en fredad sfär som den enskilde bör vara tillförsäkrad och där ett oönskat intrång, såväl psykiskt som fysiskt, bör kunna avvisas (jfr prop. 2005/06:173 s. 15). En annan aspekt på integritetsskydd är emellertid att enskilda också ska kunna kräva att staten vidtar effektiva åtgärder för att skydda hans eller hennes säkerhet. I detta ligger att staten måste vidta åtgärder för att se till att förebygga och förhindra brott. Staten har ett ansvar för att skydda enskildas liv, frihet och personliga säkerhet (jfr prop. 2015/16:167 s. 26). En väl fungerande samhällsorganisation kommer alltid att medföra vissa intrång i enskildas personliga integritet.

Kamerabevakning kan användas för att förebygga och utreda brott och har en trygghetsskapande effekt. Kamerabevakning behöver därför kunna bedrivas mer flexibelt, snabbt och resurseffektivt samt på fler platser i samhället. Det är avgörande att reglerna inte på ett omotiverat sätt hindrar polisen från att dra nytta av den teknikutveckling som har skett kopplat till kamerabevakning, t.ex. vad gäller tekniker för olika typer av automatisk igenkänning.

Nyligen genomfördes författningsändringar som underlättar användningen av teknik som innebär kamerabevakning med automatisk igenkänning av registreringsnummer i gränsnära områden (prop. 2022/23:109). Med hjälp av sådan igenkänning kan polisen följa ett fordons rörelsemönster. Informationen kan användas i syfte att förebygga, upptäcka, förhindra, utreda och lagföra brott. Med gränsnära områden avses vissa flygplatser, hamnar, järnvägsstationer, broar till andra länder och gränsövergångsställen på allmänna vägar. Teknik som innebär kamerabevakning med automatisk igenkänning av registreringsnummer skulle vara av stort värde även utanför gränsnära områden och för att bl.a. bekämpa organiserad brottslighet och terroristbrott.

Ansiktsigenkänning är ett sätt att behandla och bearbeta kamerabevakningsmaterial. En på så sätt hanterad ansiktsbild är en biometrisk uppgift och utvecklingen går mot att i allt större utsträckning använda AI-teknik för behandling och bearbetning av sådana bilder. Biometriska uppgifter får enligt artikel 10 i EU:s dataskyddsdirektiv[1] behandlas endast om det är särskilt föreskrivet och absolut nödvändigt för ändamålet med behandlingen. Detta framgår också av 2 kap. 12 § brottsdatalagen.

Enligt 1 kap. 4 § brottsdatalagen gäller lagen inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen. En bestämmelse motsvarande 2 kap. 12 § brottsdatalagen har dock tagits in även i Säkerhetspolisens datalag (se 2 kap. 10 § den lagen).

Med hänsyn till att ansiktsigenkänning utgör ett kraftfullt verktyg i kampen mot den organiserade brottsligheten är det av stor vikt att tekniken, i den utsträckning som dataskyddsdirektivet medger, kan användas effektivt och ändamålsenligt. Det finns skäl att även se över hur tekniken skulle kunna användas i större utsträckning för att bl.a. bekämpa terroristbrott och brott mot Sveriges säkerhet.

Myndigheter och andra relevanta aktörer måste ha goda förutsättningar att inhämta, behandla och utbyta information. Det finns därför ett behov av att också utreda på vilket sätt polisen på ett effektivt sätt kan få del av kamerabevakningsmaterial när det har betydelse för brottsbekämpningen.

3. Uppdraget till utredaren

3.1 Uppdraget

En utredare ges i uppdrag att se över vissa frågor kopplat till kamerabevakning. En allmän utgångspunkt för arbetet är att Polismyndighetens och Säkerhetspolisens möjligheter att använda sig och på andra sätt dra nytta av kamerabevakning behöver förbättras.

Utredaren ska analysera och lämna författningsförslag som gör att Polismyndigheten och Säkerhetspolisen i större utsträckning och på ett mer

[1] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

effektivt sätt kan använda teknik som innebär kamerabevakning med automatisk igenkänning av fordons registreringsnummer. Utredaren ska också analysera om det finns förutsättningar att låta myndigheterna i större utsträckning använda teknik som innebär kamerabevakning med automatisk ansiktsigenkänning. Utredaren ska bedöma under vilka förutsättningar som tekniken ska kunna användas i det brottsbekämpande arbetet och i förhållande till vilket kamerabevakningsmaterial. Om sådana förutsättningar finns ska utredaren lämna författningsförslag som möjliggör ett effektivt och ändamålsenligt användande av tekniken. Vidare ska utredaren analysera och lämna författningsförslag som gör att Polismyndigheten och Säkerhetspolisen i fler fall kan få ta del av kamerabevakningsmaterial från annans bevakning, t.ex. material från kamerasystem kopplade till statlig transportinfrastruktur eller från kommuner och regioners kamerabevakning.

Utredarens förslag kan innefatta utökade möjligheter att dela kamerateknik med aktörer samt samla in, använda och lagra personuppgifter. En fråga i detta sammanhang är om polisen bör ges direktåtkomst i realtid till material från annans kamerabevakning. Utredarens förslag kan även innefatta undantag från kravet att med tydlig skyltning upplysa om kamerabevakning. Förslagen ska utformas med beaktande av skyddet för den personliga integriteten liksom av EU:s dataskyddsreglering.

Utredaren får även överväga och lämna förslag i andra närliggande frågor.

Det ingår inte i utredarens uppdrag att överväga eller föreslå ändringar i bestämmelserna om hemlig kameraövervakning i 27 kap. rättegångsbalken eller i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

3.2 Utredningsarbetet

Utredaren ska under arbetet ha en dialog med och inhämta upplysningar från Integritetsskyddsmyndigheten, Polismyndigheten, Säkerhetspolisen, Trafikverket, Transportstyrelsen och Tullverket. Vid behov ska utredaren hämta in synpunkter och upplysningar även från andra relevanta aktörer och andra jämförbara länder. Utredaren ska också hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet, utredningsväsendet och EU. Som exempel kan nämnas 2023 års kamerabevakningsutredning (Ju 2023:01), Utredningen om Säkerhetspolisens informationshantering (Ju 2023:02) och regeringsuppdraget att se över Polismyndighetens

tillgång till uppgifter från befintliga kamerasystem (Ju2023/02261). Som exempel kan också nämnas förhandlingarna om den s.k. AI-förordningen (se Faktapromemoria 2020/21:FPM109).

Utredaren ska analysera och redovisa konsekvenserna av sina förslag. Vidare ska utredaren särskilt redovisa förslagens konsekvenser för den personliga integriteten samt säkerställa att förslagen är förenliga med grundläggande fri- och rättigheter, bl.a. skyddet mot betydande intrång i den personliga integriteten i 2 kap. 6 § andra stycket regeringsformen. Förslagen ska också vara förenliga med Sveriges konventionsåtaganden om mänskliga rättigheter. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna ska utredaren beräkna kostnaderna och lämna förslag om hur dessa ska finansieras.

3.3 Redovisning av uppdraget

Uppdraget ska redovisas senast den 29 maj 2024.

Europaparlamentet
2019-2024

ANTAGNA TEXTER

P9_TA(2024)0138

Rättsakten om artificiell intelligens

Europaparlamentets lagstiftningsresolution av den 13 mars 2024 om förslaget till Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))

(Ordinarie lagstiftningsförfarande: första behandlingen)

Europaparlamentet utfärdar denna resolution

– med beaktande av kommissionens förslag till Europaparlamentet och rådet (COM(2021)0206),

– med beaktande av artiklarna 294.2, 16 och 114 i fördraget om Europeiska unionens funktionssätt, i enlighet med vilka kommissionen har lagt fram sitt förslag för parlamentet (C9-0146/2021),

– med beaktande av artikel 294.3 i fördraget om Europeiska unionens funktionssätt,

– med beaktande av Europeiska centralbankens yttrande av den 29 december 2021[1],

– med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande av den 22 september 2021[2],

– med beaktande av den preliminära överenskommelse som godkänts av det ansvariga utskottet enligt artikel 74.4 i arbetsordningen och av det skriftliga åtagandet från rådets företrädare av den 2 februari 2024 att godkänna parlamentets ståndpunkt i enlighet med artikel 294.4 i fördraget om Europeiska unionens funktionssätt,

– med beaktande av artikel 59 i arbetsordningen,

– med beaktande av den gemensamma behandlingen av ärendet i utskottet för den inre marknaden och konsumentskydd och utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor, i enlighet med artikel 58 i arbetsordningen,

[1] EUT C 115, 11.3.2022, s. 5.
[2] EUT C 517, 22.12.2021, s. 56.

– med beaktande av yttrandena från utskottet för industrifrågor, forskning och energi, utskottet för kultur och utbildning, utskottet för rättsliga frågor, utskottet för miljö, folkhälsa och livsmedelssäkerhet och utskottet för transport och turism,

– med beaktande av betänkandet från utskottet för den inre marknaden och konsumentskydd och utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor (A9-0188/2023).

1. Europaparlamentet antar nedanstående ståndpunkt vid första behandlingen[3].

2. Europaparlamentet uppmanar kommissionen att på nytt lägga fram ärendet för parlamentet om den ersätter, väsentligt ändrar eller har för avsikt att väsentligt ändra sitt förslag.

3. Europaparlamentet uppdrar åt talmannen att översända parlamentets ståndpunkt till rådet, kommissionen och de nationella parlamenten.

[3] Denna ståndpunkt ersätter ändringarna antagna den 14 juni 2023 (Antagna texter, P9_TA(2023)0236).

P9_TC1-COD(2021)0106

**Europaparlamentets ståndpunkt fastställd vid första behandlingen den 13 mars 2024 inför antagandet av Europaparlamentets och rådets förordning (EU) 2024/… om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (rättsakt om artificiell intelligens)*

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 16 och 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[1],

med beaktande av Europeiska centralbankens yttrande[2],

med beaktande av Regionkommitténs yttrande[3],

i enlighet med det ordinarie lagstiftningsförfarandet[4], och

---

* TEXT HAR GENOMGÅTT PARTIELL JURISTLINGVISTISK SLUTGRANSKNING.

1 EUT C 517, 22.12.2021, s. 56.

2 ***EUT C 115, 11.3.2022, s. 5.***

3 EUT C 97, 28.2.2022, s. 60.

4 Europaparlamentets ståndpunkt av den 13 mars 2024.

av följande skäl:

(1) Syftet med denna förordning är att förbättra den inre marknadens funktionssätt genom att fastställa en enhetlig rättslig ram för i synnerhet utveckling, ***utsläppande på marknaden, ibruktagande och*** användning av ***system*** för artificiell intelligens (AI-system) ***i unionen*** i enlighet med unionens värden***, främja användningen av människocentrerad och tillförlitlig artificiell intelligens (AI) och samtidigt säkerställa*** en hög skyddsnivå för hälsa, säkerhet och grundläggande rättigheter såsom ***fastställs i Europeiska unionens stadga om de grundläggande rättigheterna (stadgan), inbegripet demokrati och rättsstatsprincipen och miljöskydd, mot skadliga effekter av AI-system i unionen, och stödja innovation***. ***Denna förordning*** säkerställer fri rörlighet över gränserna för AI-baserade varor och tjänster, och förhindrar således att medlemsstaterna inför begränsningar av utvecklingen, saluföringen och användningen av ***AI- system***, om sådana inte uttryckligen tillåts enligt denna förordning.

(2) Denna förordning bör tillämpas i enlighet med unionens värden, som fastställs i stadgan, och underlätta skyddet av fysiska personer, företag, demokratin, rättsstatsprincipen och miljöskyddet, och samtidigt främja innovation och sysselsättning och göra unionen ledande när det gäller användningen av tillförlitlig AI.

(3) ▌ AI-system ▌ kan enkelt utnyttjas inom ett stort antal olika ekonomiska sektorer och i många delar av samhället, inklusive över gränser, och kan enkelt cirkulera i hela unionen. Vissa medlemsstater har redan undersökt antagandet av nationella regler för att säkerställa att AI är ***tillförlitligt och säkert*** samt utvecklas och används i enlighet med skyldigheter som rör grundläggande rättigheter. Skiljaktiga nationella regler kan leda till fragmentering av den inre marknaden och minska rättssäkerheten för operatörer som utvecklar, ***importerar*** eller använder AI-system. En enhetlig och hög skyddsnivå bör därför säkerställas i hela unionen ***för att tillförlitlig AI ska uppnås***, medan avvikelser som hindrar den fria rörligheten för ***samt innovation inom och användning och spridning av*** AI-system och relaterade produkter och tjänster på den inre marknaden bör förhindras genom fastställande av enhetliga skyldigheter för operatörer och garanterande av ett enhetligt skydd för tvingande hänsyn till allmänintresset och personers rättigheter på hela den inre marknaden på grundval av artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget). I den utsträckning som denna förordning omfattar särskilda regler för skydd av individer när det gäller behandling av personuppgifter avseende begränsning av användningen av AI-system för biometrisk fjärridentifiering ***för brottsbekämpningsändamål, av användningen av AI-system för riskbedömningar av fysiska personer för brottsbekämpningsändamål och av användningen av AI-system för biometrisk kategorisering*** för brottsbekämpningsändamål, är det, när det gäller dessa särskilda regler, lämpligt att grunda denna förordning på artikel 16 i EUF-fördraget. Mot bakgrund av dessa särskilda regler och användningen av artikel 16 i EUF-fördraget är det lämpligt att samråda med Europeiska dataskyddsstyrelsen.

(4) AI ingår i en teknikfamilj under snabb utveckling som ***bidrar*** till en mängd ekonomiska, ***miljömässiga*** och samhälleliga vinster över hela spektrumet av näringslivssektorer och samhällsverksamheter. Genom att förbättra förutsägelserna, optimera verksamheter och resurstilldelning och individanpassa de digitala lösningar som är tillgängliga för enskilda och organisationer kan användningen av AI ge företagen viktiga konkurrensfördelar och stödja socialt och miljömässigt fördelaktiga utfall, exempelvis inom hälso- och sjukvård, jordbruk, ***livsmedelssäkerhet***, utbildning, ***medier, sport, kultur,*** infrastrukturförvaltning, energi, transport och logistik, offentliga tjänster, säkerhet, rättsväsen, resurs- och energieffektivitet. ***miljöövervakning, bevarande och återställande av biologisk mångfald och ekosystem*** samt begränsning av och anpassning till klimatförändringar.

(5) Samtidigt kan AI, beroende på omständigheterna kring den specifika tillämpningen***, användningen och den tekniska utvecklingsnivån***, ge upphov till risker och skada allmänna intressen och ***grundläggande*** rättigheter som skyddas av unionsrätten. Dessa skador kan vara materiella eller immateriella***, inbegripet fysiska, psykologiska, samhälleliga eller ekonomiska skador***.

(6) Med tanke på den stora inverkan som AI kan ha på samhället, och behovet av att bygga upp förtroende, är det mycket viktigt att AI och dess regelverk utvecklas i enlighet med unionens värden såsom de fastställs i artikel 2 i fördraget om Europeiska unionen (EU-fördraget), de grundläggande rättigheter och friheter som fastställs i fördragen och, i enlighet med artikel 6 i EU-fördraget, stadgan. En förutsättning är att AI bör vara en människocentrerad teknik. Den bör fungera som ett verktyg för människor, med slutmålet att öka människors välbefinnande.

(7) För att säkerställa en konsekvent och hög skyddsnivå för allmänintressen på områdena hälsa, säkerhet och grundläggande rättigheter bör gemensamma regler fastställas för AI-system med hög risk. Dessa regler bör vara förenliga med stadgan. icke-diskriminerande och i linje med unionens internationella handelsåtaganden. De bör också ta hänsyn till den europeiska förklaringen om digitala rättigheter och principer för det digitala decenniet och de etiska riktlinjerna för tillförlitlig AI från högnivåexpertgruppen för artificiell intelligens (AI-expertgruppen).

(8) Därmed behövs en rättslig ram för unionen som fastställer harmoniserade regler för AI för att främja utvecklingen, användningen och spridningen av AI på den inre marknaden, varigenom samtidigt en hög skyddsnivå uppnås för allmänintressen, såsom hälsa, säkerhet och skydd av grundläggande rättigheter***, inbegripet demokrati, rättsstatsprincipen och miljöskydd,*** såsom erkänns och skyddas enligt unionsrätten. För att uppnå detta syfte bör det fastställas regler som reglerar utsläppandet på marknaden, ibruktagandet ***och användningen*** av vissa AI-system, för att på så sätt säkerställa en fungerande inre marknad och göra det möjligt för dessa system att omfattas av principen om fri rörlighet för varor och tjänster. ***Dessa regler bör vara tydliga och robusta när det gäller att skydda de grundläggande rättigheterna, stödja nya innovativa lösningar, möjliggöra ett europeiskt ekosystem av offentliga och privata aktörer som skapar AI-system i linje med unionens värden och ta tillvara den digitala omställningens potential i hela unionen.*** Genom fastställandet av dessa regler***, och åtgärder till stöd för innovation med särskild inriktning på små och medelstora företag, inbegripet uppstartsföretag,*** stöder denna förordning unionens mål att ***främja den europeiska människocentrerade AI-strategin*** och att bli världsledande inom utvecklingen av säker, tillförlitlig och etisk AI [redacted], såsom fastställts av Europeiska rådet[5], och den säkerställer skyddet av etiska principer, vilket särskilt har begärts av Europaparlamentet[6].

[5] Europeiska rådet, extra möte i Europeiska rådet (den 1 och 2 oktober 2020) – Slutsatser, EUCO 13/20, 2020, s. 6.

[6] Europaparlamentets resolution av den 20 oktober 2020 med rekommendationer till kommissionen om en ram för etiska aspekter av artificiell intelligens, robotteknik och tillhörande teknik (2020/2012(INL)).

(9) Harmoniserade regler som är tillämpliga på utsläppande på marknaden, ibruktagande och användning av AI-system med hög risk bör fastställas i enlighet med Europaparlamentets och rådets förordning (EG) nr 765/2008[7], Europaparlamentets och rådets beslut nr 768/2008/EG[8] och Europaparlamentets och rådets förordning (EU) 2019/1020[9](*den nya lagstiftningsramen*). ***De harmoniserade regler som fastställs i denna förordning bör gälla i alla sektorer och bör, i linje med den nya lagstiftningsramen, inte påverka befintlig unionslagstiftning, särskilt om dataskydd, konsumentskydd, grundläggande rättigheter, sysselsättning och skyddet av arbetstagare, samt produktsäkerhet, vilken denna förordning kompletterar.***

[7] Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

[8] Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG (EUT L 218, 13.8.2008, s. 82).

[9] Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011 (Text av betydelse för EES) (EUT L 169, 25.6.2019, s. 1).

Alla rättigheter och rättsmedel som föreskrivs genom sådan unionslagstiftning för konsumenter, och andra personer som AI-system kan ha en negativ inverkan på, inbegripet när det gäller ersättning för eventuella skador enligt rådets direktiv 85/374/EEG[10], förblir som en följd av detta opåverkade och fullt tillämpliga. Vidare bör denna förordning, när det gäller anställning och skydd av arbetstagare, därför inte påverka unionsrätten om socialpolitik och nationell arbetsrätt, i enlighet med unionsrätten, om anställnings- och arbetsvillkor, inbegripet hälsa och säkerhet på arbetsplatsen och förhållandet mellan arbetsgivare och arbetstagare. Denna förordning bör inte heller påverka utövandet av de grundläggande rättigheter som erkänns i medlemsstaterna och på unionsnivå, inbegripet rätten eller friheten att strejka eller att vidta annan åtgärd som ingår i medlemsstaternas respektive arbetsmarknadsmodell, eller rätten att förhandla om, ingå och tillämpa kollektivavtal eller vidta kollektiva åtgärder i enlighet med nationell rätt.

[10] Rådets direktiv 85/374/EEG av den 25 juli 1985 om tillnärmning av medlemsstaternas lagar och andra författningar om skadeståndsansvar för produkter med säkerhetsbrister (EGT L 210, 7.8.1985, s. 29).

Denna förordning bör inte påverka de bestämmelser som syftar till att förbättra arbetsvillkoren för plattformsarbete och som fastställs i Europaparlamentets och rådets direktiv (EU) 2024/...[11+]. Dessutom syftar denna förordning till att stärka effektiviteten hos sådana befintliga rättigheter och rättsmedel genom att särskilda krav och skyldigheter fastställs, bland annat när det gäller transparens, teknisk dokumentation och arkivering avseende AI-system. Vidare bör de skyldigheter som åläggs olika operatörer som ingår i AI-värdekedjan enligt denna förordning tillämpas utan att det påverkar nationell rätt i enlighet med unionsrätten, med verkan att användningen av vissa AI-system begränsas när sådan lagstiftning inte omfattas av denna förordning eller eftersträvar andra legitima mål av allmänt intresse än dem som eftersträvas genom denna förordning. Till exempel bör nationell arbetsrätt och lagstiftningen om skydd av minderåriga, dvs. personer under 18 år, med beaktande av FN:s allmänna kommentar nr 25 (2021) om barns rättigheter i den digitala miljön, i den mån de inte är specifika för AI-system och eftersträvar andra legitima mål av allmänt intresse, inte påverkas av denna förordning.

---

11 Europaparlamentets och rådets direktiv (EU) 2024/... av den... om bättre arbetsvillkor för plattformsarbete (EUT L,..., ELI: …).

\+ För in numret på direktivet i PE XX/YY (2021/0414 (COD)) i texten och komplettera fotnoten.

(10) Den grundläggande rätten till skydd av personuppgifter garanteras särskilt genom Europaparlamentets och rådets förordningar (EU) 2016/679[12] och (EU) 2018/1725[13] samt Europaparlamentets och rådets direktiv (EU) 2016/680[14]. Europaparlamentets och rådets direktiv 2002/58/EG[15] skyddar dessutom privatlivet och konfidentialitet vid kommunikation, bland annat genom att villkor föreskrivs för all lagring av personuppgifter och icke-personuppgifter i terminalutrustning och för åtkomst från terminalutrustning. Dessa unionsrättsakter ger grunden för en hållbar och ansvarsfull databehandling, även i de fall då dataset innehåller en blandning av personuppgifter och icke-personuppgifter. Denna förordning syftar inte till att påverka tillämpningen av befintlig unionslagstiftning om behandling av personuppgifter, inbegripet uppgifter och befogenheter för de oberoende tillsynsmyndigheter som är behöriga att övervaka efterlevnaden av dessa instrument.

---

12 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

13 Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

14 Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).

15 Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (Direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

Den påverkar inte heller de skyldigheter som leverantörer och spridare av AI-system har i sin roll som personuppgiftsansvariga eller personuppgiftsbiträden enligt unionsrätten eller nationell rätt om skydd av personuppgifter, i den mån utformningen, utvecklingen eller användningen av AI-system inbegriper behandling av personuppgifter. Det är också lämpligt att klargöra att registrerade fortsätter att åtnjuta alla de rättigheter och garantier som de tillerkänns genom sådan unionslagstiftning, inbegripet de rättigheter som rör uteslutande automatiserat individuellt beslutsfattande, inbegripet profilering. Harmoniserade regler för utsläppande på marknaden, ibruktagande och användning av AI-system som inrättas enligt denna förordning bör underlätta ett effektivt genomförande och göra det möjligt för de registrerade att utöva sina rättigheter och andra rättsmedel som garanteras enligt unionsrätten om skydd av personuppgifter och av andra grundläggande rättigheter.

(11) Denna förordning bör inte påverka tillämpningen av bestämmelserna om tjänstelevererande mellanhänders ansvar enligt Europaparlamentets och rådets direktiv 2000/31/EG[16].

[16] Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (”Direktiv om elektronisk handel”) (EGT L 178, 17.7.2000, s. 1).

(12) Begreppet *AI-system* ***i denna förordning*** bör vara tydligt definierat och ***nära anpassat till det arbete som utförs av internationella organisationer som arbetar med AI*** för att säkerställa rättssäkerhet, ***underlätta internationell konvergens och bred acceptans,*** och samtidigt ge flexibilitet för att hantera ***den snabba*** tekniska utvecklingen ***på detta område***. ***Dessutom*** bör ***det*** baseras på ***centrala*** egenskaper hos ***AI-system som skiljer det från enklare traditionella programvarusystem eller programmeringsmetoder och inte omfatta system som bygger på de regler som endast fysiska personer fastställer för att automatiskt utföra operationer***. ***En viktig egenskap hos AI-system är deras förmåga att dra slutsatser. Denna slutsatsförmåga avser processen att erhålla*** utdata, såsom ***förutsägelser, innehåll***, rekommendationer eller beslut, som ***kan*** påverka ***fysiska och virtuella miljöer och AI-systemens förmåga att härleda modeller eller algoritmer från indata eller data***. ***De tekniker som gör inferens möjlig när man bygger upp ett AI-system inbegriper metoder för maskininlärning för inlärning genom data om hur man uppnår vissa mål och logik- och kunskapsbaserade strategier som drar slutsatser av kodad kunskap om eller symbolisk representation av den uppgift som ska lösas. Ett AI-systems kapacitet att dra slutsatser går utöver grundläggande databehandling och möjliggör inlärning, resonemang eller modellering. Termen ”maskinbaserad” avser det faktum att AI-system körs på maskiner.***

Hänvisningen till uttryckliga eller underförstådda mål understryker att AI-system kan fungera enligt uttryckliga definierade mål eller underförstådda mål. AI-systemets ***mål kan skilja sig från AI-systemets avsedda ändamål i ett*** specifikt ***sammanhang****. Vid tillämpningen av denna förordning* bör ***miljöer förstås som de sammanhang där AI-systemen är i drift, medan utdata som genereras av AI-systemet återspeglar olika funktioner som utförs av AI-system och inbegriper förutsägelser, innehåll, rekommendationer eller beslut. AI-system är utformade för att fungera med varierande grad av autonomi, vilket innebär att de är oberoende av mänsklig kontroll i viss mån och har förmåga att fungera utan mänskligt ingripande. Den anpassningsförmåga som ett AI-system kan uppvisa när det införts avser förmågan till självlärande, vilket gör det möjligt för systemet att förändras under sin användning. AI-system kan användas fristående eller som komponent i en produkt, oavsett om systemet är fysiskt integrerat i produkten (inbyggt) eller tjänar produktens funktioner utan att vara integrerat i produkten (ej inbyggt).***

(13) Begreppet spridare, som det hänvisas till i denna förordning, bör tolkas som varje fysisk eller juridisk person, inbegripet en offentlig myndighet, offentlig byrå eller ett annat organ, som under eget överinseende använder ett AI-system, med undantag för om AI-systemet används under personlig icke-yrkesmässig verksamhet. Beroende på typen av AI-system kan användningen av systemet påverka andra personer än spridaren.

(14) Begreppet *biometriska uppgifter* som används i denna förordning ▌ bör tolkas ***mot bakgrund av*** begreppet biometriska uppgifter enligt definitionen i artikel 4.14 i förordning (EU) 2016/679, artikel 3.18 i förordning (EU) 2018/1725 och artikel 3.13 i direktiv (EU) 2016/680. ***Biometriska uppgifter kan ge möjlighet till autentisering, identifiering och kategorisering av fysiska personer och igenkänning av fysiska personers känslor***

(15) Begreppet biometrisk identifiering, som det hänvisas till i denna förordning, bör definieras som automatiserad igenkänning av fysiska, fysiologiska och beteendemässiga mänskliga särdrag såsom ansikte, ögonrörelser, kroppsform, röst, prosodi, gång, hållning, hjärtfrekvens, blodtryck, lukt eller tangenttryckningskarakteristik för att fastställa en enskild persons identitet genom att jämföra denna individs biometriska uppgifter med lagrade biometriska uppgifter tillhörande individer i en referensdatabas, oavsett om individen har givit sitt medgivande eller inte. Detta utesluter AI-system som är avsedda att användas för biometrisk verifiering, vilket inbegriper autentisering, vars enda syfte är att bekräfta att en specifik fysisk person är den person som denne utger sig för att vara att bekräfta identiteten för en fysisk person med det enda syftet att få åtkomst till en tjänst, låsa upp en enhet eller ha säker tillgång till lokaler.

(16) Begreppet biometrisk kategorisering, som det hänvisas till i denna förordning, bör definieras som att fysiska personer hänförs till särskilda kategorier på grundval av deras biometriska uppgifter. Sådana särskilda kategorier kan avse aspekter som kön, ålder, hårfärg, ögonfärg, tatueringar, beteende- eller personlighetsdrag, språk, religion, tillhörighet till nationell minoritet eller sexuell eller politisk läggning. Detta omfattar inte system för biometrisk kategorisering som har en ren extrafunktion som är oupplösligt kopplad till en annan kommersiell tjänst, vilket innebär att funktionen av objektiva tekniska skäl inte kan användas utan den huvudsakliga tjänsten och att integreringen av denna funktion inte är ett sätt att kringgå tillämpligheten av bestämmelserna i denna förordning. Filter som kategoriserar ansikts- eller kroppsegenskaper som används på e-marknadsplatser kan till exempel utgöra en sådan extrafunktion, eftersom de kan användas endast i förhållande till den huvudsakliga tjänsten, som är att sälja en produkt genom att göra det möjligt för konsumenten att i förväg se produkten på sig själv och hjälpa konsumenten att fatta ett köpbeslut. Filter som används på sociala nätverkstjänster online och som kategoriserar ansikts- eller kroppsfunktioner för att göra det möjligt för användare att lägga till eller ändra bilder eller videor kan också betraktas som extrafunktioner, eftersom ett sådant filter inte kan användas utan den huvudsakliga tjänsten hos de sociala nätverkstjänsterna som utgörs av delning av innehåll online.

(17) Begreppet *system för biometrisk fjärridentifiering*, som det hänvisas till i denna förordning, bör definieras utifrån funktion som ett AI-system avsett för identifiering av fysiska personer ***utan deras aktiva medverkan, vanligtvis*** på distans, genom jämförelse mellan en persons biometriska uppgifter och biometriska uppgifter i en referensdatabas, ***oavsett den specifika teknik, process eller typ av biometriska uppgifter som används***. ***Sådana system för biometrisk fjärridentifiering används vanligtvis för att samtidigt uppfatta flera personer eller deras beteende för att avsevärt underlätta identifieringen av fysiska personer*** utan ***deras aktiva medverkan***. ***Detta utesluter AI-system som är avsedda att användas för biometrisk verifiering, vilket inbegriper autentisering, vars enda syfte är att bekräfta att en specifik fysisk person är den person som denne utger sig för att vara, och system som används för att bekräfta identiteten för en fysisk person med det enda syftet att få åtkomst till en tjänst, låsa upp en enhet eller ha säker tillgång till lokaler. Detta uteslutande motiveras av att sådana system sannolikt har mindre inverkan på fysiska personers grundläggande rättigheter än de system för biometrisk fjärridentifiering som kan användas för behandling av*** biometriska ***uppgifter om ett stort antal personer utan deras aktiva medverkan.*** När det gäller system i realtid sker insamlingen av biometriska uppgifter, jämförelsen och identifieringen omedelbart, näst intill omedelbart eller under alla omständigheter utan betydande dröjsmål. I detta avseende bör det inte finnas något utrymme för att kringgå denna förordnings regler om användning i realtid av de berörda AI-systemen genom att medge mindre fördröjningar. Realtidssystem involverar direktupptagningar eller näst intill direktupptagningar av material, såsom videoupptagningar, genererade med kamera eller annan utrustning med liknande funktion. Efterhandssystem baseras däremot på redan insamlade biometriska uppgifter och jämförelsen och identifieringen sker med en betydande fördröjning. Detta involverar sådant material som bilder eller videoupptagningar som genereras genom övervakningskameror (CCTV) eller privat utrustning och som har genererats före användningen av systemet vad gäller de berörda fysiska personerna.

(18) Begreppet system för känsloigenkänning, som det hänvisas till i denna förordning, bör definieras som ett AI-system vars syfte är att identifiera eller uttyda fysiska personers känslor eller avsikter på grundval av deras biometriska uppgifter. Begreppet avser känslor eller avsikter som lycka, sorg, ilska, överraskning, avsky, förlägenhet, sinnesrörelse, skam, förakt, nöjdhet och förnöjelse. Det omfattar inte fysiska tillstånd, såsom smärta eller trötthet; detta avser till exempel system som används för att upptäcka trötthetstillståndet hos yrkespiloter eller yrkeschaufförer i syfte att förebygga olyckor. Detta omfattar inte heller enbart upptäckt av lätt skönjbara uttryck, gester eller rörelser, såvida de inte används för att identifiera eller dra slutsatser om känslor. De uttrycken kan vara grundläggande ansiktsuttryck såsom en sur min eller ett leende, eller gester som rörelser av händer, armar eller huvud, eller egenskaper hos en persons röst, till exempel höjd röst eller viskningar.

(19) I denna förordning bör begreppet *allmänt tillgänglig plats* förstås som varje fysisk plats som är tillgänglig för ***ett obestämt antal fysiska personer och*** oberoende av om platsen i fråga är privatägd eller offentligägd***, oberoende av den verksamhet för vilken platsen får användas, såsom handel (t.ex. affärer, restauranger, kaféer), tjänster (t.ex. banker, yrkesverksamhet, besöksnäring). idrott (t.ex. simbassänger, gym, arenor), transport (t.ex. buss-, tunnelbane- och järnvägsstationer, flygplatser, transportmedel), underhållning (t.ex. biografer, teatrar, museer, konsert- och konferenslokaler), fritid eller annat (t.ex. allmänna vägar och torg, parker, skogar, lekplatser). En plats bör klassificeras som allmänt tillgänglig även om tillträdet, oavsett potentiella kapacitets- eller säkerhetsbegränsningar, omfattas av*** vissa ***på förhand fastställda*** villkor ***som kan uppfyllas av ett obestämt antal personer,*** såsom ***köp av en biljett, förhandsregistrering eller en viss ålder. Däremot bör en plats inte anses vara allmänt tillgänglig om åtkomsten är begränsad till specifika och definierade fysiska personer antingen genom unionslagstiftning eller nationell lagstiftning med direkt anknytning till allmän säkerhet eller säkerhet eller genom att den person som har relevant befogenhet på platsen tydligt uttrycker sin vilja. Den faktiska möjligheten till tillträde (t.ex. en olåst dörr, en öppen grind i ett stängsel) innebär*** inte att ***platsen är*** allmänt tillgänglig ***om det finns indikationer eller omständigheter som tyder på motsatsen (t.ex. skyltar som förbjuder eller begränsar tillträdet). Företags- och fabrikslokaler samt kontor och arbetsplatser till vilka avsikten är att endast*** berörda ***anställda och tjänsteleverantörer ska ha tillträde är platser som inte är allmänt tillgängliga. Allmänt tillgängliga platser bör inte omfatta fängelser eller gränskontrollområden. Vissa andra områden kan bestå av både områden som inte är allmänt tillgängliga och områden som är allmänt tillgängliga,*** såsom ***en korridor i ett privat bostadshus som krävs för tillträde till en läkarmottagning eller en flygplats. Onlineplatser omfattas inte heller eftersom de inte är fysiska platser.*** Det bör dock avgöras från fall till fall om en viss plats är tillgänglig för allmänheten, med beaktande av den individuella situationens särdrag.

(20) För att dra största möjliga nytta av AI-system och samtidigt skydda grundläggande rättigheter, hälsa och säkerhet och möjliggöra demokratisk kontroll bör AI-kunskap förse leverantörer, spridare och berörda personer med de begrepp som krävs för att fatta välgrundade beslut om AI-system. Dessa begrepp kan variera med avseende på det relevanta sammanhanget och kan inbegripa förståelse av den korrekta tillämpningen av tekniska delar under AI-systemets utvecklingsfas, de åtgärder som ska tillämpas under dess användning, lämpliga sätt att tolka AI-systemets utdata och, när det gäller berörda personer, den kunskap som krävs för att förstå hur beslut som fattas med hjälp av AI kommer att påverka dem. I samband med tillämpningen av denna förordning bör AI-kunskap ge alla relevanta aktörer i AI-värdekedjan de insikter som krävs för att säkerställa lämplig efterlevnad och korrekt verkställighet. Dessutom kan ett brett genomförande av åtgärder för AI-kunskap och införandet av lämpliga uppföljningsåtgärder bidra till att förbättra arbetsvillkoren och i slutändan upprätthålla konsolideringen av och innovationsbanan för tillförlitlig AI i unionen. Den europeiska nämnden för artificiell intelligens (nämnden) bör stödja kommissionen för att främja AI-kunskap, allmänhetens medvetenhet om och förståelse av fördelar, risker, skyddsåtgärder, rättigheter och skyldigheter i samband med användningen av AI-system. I samarbete med berörda parter bör kommissionen och medlemsstaterna underlätta utarbetandet av frivilliga uppförandekoder för att öka AI-kunskapen hos personer som arbetar med utveckling, drift och användning av AI.

(21) För att säkerställa lika villkor och ett effektivt skydd av individers rättigheter och friheter i hela unionen bör de regler som fastställs genom denna förordning tillämpas på leverantörer av AI-system på ett icke-diskriminerande sätt, oavsett om de är etablerade i unionen eller i ett tredjeland, och på ***spridare*** av AI-system som är etablerade i unionen.

(22) Mot bakgrund av AI-systemens digitala natur bör vissa AI-system omfattas av denna förordning även om de inte släpps ut på marknaden, tas i bruk eller används i unionen. Detta är exempelvis fallet om en operatör som är etablerad i unionen lägger ut vissa tjänster på entreprenad hos en operatör som är etablerad i ett tredjeland i fråga om en aktivitet som ska utföras av ett AI-system som skulle klassificeras som hög risk ▌ . Under dessa omständigheter kan det AI-system som används i ett tredjeland av operatören behandla data som på lagligt sätt samlats in och överförts från unionen och förse den avtalsslutande operatören i unionen med utdata från detta AI-system som är resultatet av denna behandling, utan att det berörda AI-systemet släppts ut på marknaden, tagits i bruk eller använts i unionen. För att förhindra att denna förordning kringgås och säkerställa ett effektivt skydd av fysiska personer som befinner sig i unionen, bör förordningen också tillämpas på leverantörer och ***spridare*** av AI-system som är etablerade i tredjeländer, i den utsträckning som de utdata som produceras av dessa AI-system ***är avsedda att*** användas i unionen.

För att ta hänsyn till befintliga arrangemang och särskilda behov av ***framtida*** samarbete med utländska partner med vilka information och bevis utbyts, bör denna förordning dock inte tillämpas på offentliga myndigheter i tredjeländer eller internationella organisationer som agerar inom ramen för ***samarbete eller*** internationella avtal som ingåtts på unionsnivå eller nationell nivå och som avser brottsbekämpande och rättsligt samarbete med unionen eller medlemsstaterna***, förutsatt att det tredjeland eller de internationella organisationer som berörs erbjuder tillräckliga skyddsåtgärder vad avser skyddet av enskildas grundläggande rättigheter och friheter***. ***I relevanta fall kan detta omfatta verksamhet som bedrivs av enheter som av tredjeländerna fått i uppdrag att utföra särskilda uppgifter till stöd för sådant brottsbekämpande och rättsligt samarbete. Sådana ramar för samarbete eller*** avtal har ***fastställts*** bilateralt mellan medlemsstater och tredjeländer eller mellan Europeiska unionen, Europol och andra unionsbyråer och tredjeländer och internationella organisationer. ***De myndigheter som är behöriga att utöva tillsyn över brottsbekämpande och rättsliga myndigheter enligt denna förordning bör bedöma huruvida dessa ramar för samarbete eller internationella avtal innehåller lämpliga skyddsåtgärder med avseende på skyddet av enskildas grundläggande rättigheter och friheter. De av mottagarmyndigheterna i medlemsstaterna och av unionens institutioner, byråer och organ som använder sådana utdata i unionen förblir ansvariga för att säkerställa att användningen av dessa är förenlig med unionsrätten. När dessa internationella avtal ses över eller när nya ingås i framtiden bör de avtalsslutande parterna göra sitt yttersta för att anpassa dessa avtal till kraven i denna förordning.***

(23) Denna förordning bör också tillämpas på unionens institutioner, organ och byråer när de agerar som leverantör eller ***spridare*** av ett AI-system. ▌

(24) Om och i den mån AI-system släpps ut på marknaden, tas i bruk eller används med eller utan ändringar av sådana system för militära ändamål, försvarsändamål eller ändamål som rör nationell säkerhet, bör dessa utesluts från denna förordnings tillämpningsområde, oavsett vilken typ av enhet som bedriver denna verksamhet, t.ex. en offentlig eller privat enhet. När det gäller militära ändamål och försvarsändamål motiveras ett sådant uteslutande både av artikel 4.2 i EU-fördraget och av särdragen i medlemsstaternas och unionens gemensamma försvarspolitik som omfattas av kapitel 2 i avdelning V i EU-fördraget och som omfattas av folkrätten, som därför är den lämpligaste rättsliga ramen för reglering av AI-system i samband med användning av dödligt våld och andra AI-system inom ramen för militär verksamhet och försvarsverksamhet. När det gäller ändamål som rör nationell säkerhet motiveras uteslutandet både av att den nationella säkerheten helt och hållet faller under medlemsstaternas ansvarsområde i enlighet med artikel 4.2 i EU-fördraget och av den särskilda karaktär och de operativa behov som verksamheten avseende den nationella säkerheten har samt av de särskilda nationella bestämmelser som är tillämpliga på denna verksamhet. Om ett AI-system som utvecklas, släpps ut på marknaden, tas i bruk eller används för militära ändamål, försvarsändamål eller ändamål som rör nationell säkerhet tillfälligt eller permanent används för andra ändamål, t.ex. civila eller humanitära ändamål, eller ändamål som rör brottsbekämpning eller allmän säkerhet, ska ett sådant system ändå omfattas av denna förordning.

I så fall bör den enhet som använder systemet för andra ändamål än militära ändamål, försvarsändamål eller ändamål som rör nationell säkerhet säkerställa att systemet överensstämmer med denna förordning, såvida inte systemet redan är förenligt med denna förordning. AI-system som släpps ut på marknaden eller tas i bruk för ett ändamål som är uteslutet, dvs. militärt eller som rör försvar eller nationell säkerhet, och ett eller flera icke-uteslutna ändamål, såsom civila ändamål eller brottsbekämpning, omfattas av denna förordning, och leverantörer av dessa system bör säkerställa efterlevnad av denna förordning. I dessa fall bör det faktum att ett AI-system kan omfattas av denna förordning inte påverka möjligheten för enheter som bedriver verksamhet inom nationell säkerhet, försvarsverksamhet och militär verksamhet, oavsett vilken typ av enhet som bedriver denna verksamhet, att använda AI-system för nationell säkerhet, militära ändamål och försvarsändamål, vars användning är undantagen från denna förordnings tillämpningsområde. Ett AI-system som släpps ut på marknaden för civila ändamål eller brottsbekämpningsändamål och som används med eller utan ändringar för militära ändamål, försvarsändamål eller ändamål som rör nationell säkerhet bör inte omfattas av denna förordning, oavsett vilken typ av enhet som utför denna verksamhet.

(25) Denna förordning bör stödja innovation, respektera forskningsfriheten och inte underminera forsknings- och utvecklingsverksamhet. Det är därför nödvändigt att från dess tillämpningsområde undanta AI-system och AI-modeller som särskilt utvecklats och tagits i bruk enbart för vetenskaplig forskning och utveckling. Det är dessutom nödvändigt att säkerställa att denna förordning inte på annat sätt påverkar vetenskaplig forsknings- och utvecklingsverksamhet avseende AI-system eller AI-modeller innan dessa släpps ut på marknaden eller tas i bruk. Inte heller när det gäller produktorienterad forsknings-, testnings- och utvecklingsverksamhet för AI-system eller AI-modeller bör bestämmelserna i denna förordning tillämpas innan dessa system och modeller tas i bruk eller släpps ut på marknaden. Detta uteslutande påverkar inte skyldigheten att följa denna förordning om ett AI-system som faller inom tillämpningsområdet för denna förordning släpps ut på marknaden eller tas i bruk till följd av sådan forsknings- och utvecklingsverksamhet eller tillämpningen av bestämmelser om regulatoriska sandlådor och testning under verkliga förhållanden. Utan att det påverkar tillämpningen av uteslutandet när det gäller AI-system som särskilt utvecklats och tagits i bruk enbart för vetenskaplig forskning och utveckling bör alla andra AI-system som kan användas för att genomföra forsknings- och utvecklingsverksamhet även fortsättningsvis omfattas av bestämmelserna i denna förordning. All forsknings- och utvecklingsverksamhet bör i vilket fall genomföras i enlighet med erkända etiska och yrkesmässiga standarder för vetenskaplig forskning och bör bedrivas i enlighet med tillämplig unionslagstiftning.

(26) För att införa en proportionerlig och effektiv uppsättning bindande regler för AI-system bör en tydligt definierad riskbaserad metod användas. Denna metod bör innebära att dessa reglers art och innehåll anpassas till intensiteten och omfattningen av de risker som AI-systemen kan generera. Det är därför nödvändigt att förbjuda vissa ***oacceptabla*** AI-metoder, fastställa vissa krav för AI-system med hög risk och skyldigheter för berörda operatörer samt fastställa transparensskyldigheter för vissa AI-system.

(27) Den riskbaserade metoden utgör grunden för en proportionerlig och effektiv uppsättning bindande regler, men det är viktigt att påminna om de etiska riktlinjer för tillförlitlig AI från 2019 som utarbetats av den oberoende AI-expertgruppen, som utsetts av kommissionen. I dessa riktlinjer utarbetade AI-expertgruppen sju icke-bindande etiska principer för AI som bör bidra till att säkerställa att AI är tillförlitlig och etiskt sund. De sju principerna omfattar mänskligt agentskap och mänsklig tillsyn, teknisk robusthet och säkerhet, integritet och dataförvaltning, transparens, mångfald, icke-diskriminering och rättvisa, samhällets och miljöns välbefinnande samt ansvarsskyldighet. Utan att det påverkar de rättsligt bindande kraven i denna förordning och annan tillämplig unionsrätt bidrar dessa riktlinjer till utformningen av en konsekvent, tillförlitlig och människocentrerad AI, i linje med stadgan och de värden som unionen bygger på. Enligt AI-expertgruppens riktlinjer innebär mänskligt agentskap och mänsklig tillsyn att AI-system utvecklas och används som ett verktyg som tjänar människor, respekterar mänsklig värdighet och personlig självständighet och ska fungera så att de på ett lämpligt sätt kan kontrolleras och övervakas av människor.

Teknisk robusthet och säkerhet innebär att AI-system ska utvecklas och användas på ett sätt som möjliggör robusthet i händelse av problem och resiliens mot försök att ändra AI-systemets användning eller prestanda för att möjliggöra olaglig användning från tredje parters sida, och minimerar oavsiktlig skada. Integritet och dataförvaltning innebär att AI-system utvecklas och används i enlighet med integritets- och dataskyddsregler, samtidigt som data som uppfyller höga standarder i fråga om kvalitet och integritet behandlas. Transparens innebär att AI-system utvecklas och används på ett sätt som möjliggör lämplig spårbarhet och förklarbarhet, samtidigt som människor informeras om att de kommunicerar eller interagerar med ett AI-system och spridarna vederbörligen informeras om AI-systemets kapacitet och begränsningar och personer som påverkas informeras om sina rättigheter. Mångfald, icke-diskriminering och rättvisa innebär att AI-system utvecklas och används på ett sätt som inkluderar olika aktörer och främjar lika tillgång, jämställdhet och kulturell mångfald, samtidigt som man undviker diskriminerande effekter och oskäliga snedvridningar som är förbjudna enligt unionsrätten eller nationell rätt. Samhällets och miljöns välbefinnande innebär att AI-system utvecklas och används på ett hållbart och miljövänligt sätt samt för att gynna alla människor, samtidigt som man övervakar och bedömer de långsiktiga effekterna för individen, samhället och demokratin. Tillämpningen av dessa principer bör, när så är möjligt, omsättas i utformningen och användningen av AI-modeller. De bör under alla omständigheter ligga till grund för utarbetandet av uppförandekoder inom ramen för denna förordning. Alla berörda parter, inbegripet industrin, den akademiska världen, det civila samhället och standardiseringsorganisationer, uppmanas att på lämpligt sätt beakta de etiska principerna för utveckling av frivillig bästa praxis och standarder.

(28) Vid sidan av de många nyttiga användningsområdena för AI kan tekniken också användas felaktigt och tillhandahålla nya och kraftfulla verktyg för manipulation, utnyttjande och social kontroll. Sådana metoder är särskilt skadliga och ***kränkande och*** bör förbjudas eftersom de strider mot unionens värden och respekten för människans värdighet, frihet, jämlikhet, demokrati och rättsstatsprincipen och grundläggande rättigheter som fastställs i stadgan, inbegripet rätten till icke-diskriminering, dataskydd och personlig integritet samt barnets rättigheter.

(29) ***AI-baserad manipulativ teknik kan användas för att övertyga personer att ägna sig åt oönskat beteende, eller för att vilseleda dem genom att puffa dem till beslut på ett sätt som undergräver och försämrar deras autonomi, beslutsfattande och fria val.*** Utsläppandet på marknaden, ibruktagandet eller användningen av vissa AI-system ***med målet eller följden att*** det mänskliga beteendet ***väsentligt snedvrids*** och som sannolikt kan medföra ***betydande skador, i synnerhet med tillräckligt betydande negativa konsekvenser*** för den fysiska ***eller psykiska hälsan eller ekonomiska intressen***, ***är särskilt farliga och*** bör ***därför*** förbjudas. Sådana AI-system utnyttjar subliminala komponenter ***såsom ljud-, bild- och videostimuli som människor*** inte kan uppfatta ***eftersom dessa stimuli ligger utanför människans uppfattningsförmåga eller annan manipulativ eller vilseledande teknik som undergräver eller försämrar människors autonomi, beslutsfattande eller fria val på ett sätt som människor inte är medvetna om, eller om de är medvetna om det, fortfarande vilseleds eller inte kan kontrollera eller stå emot. Detta kan underlättas av till exempel maskin–hjärna-gränssnitt eller virtuell verklighet eftersom det möjliggör en högre grad av kontroll av vilka stimuli som personer utsätts för, i den mån som de väsentligt kan snedvrida deras beteende på ett betydande skadligt sätt. Dessutom kan AI-system också på annat sätt*** utnyttja sårbarheterna hos ***en person eller en viss grupp av personer*** på grund av ålder, ***funktionsnedsättning i den mening som avses i Europaparlamentets och rådets direktiv (EU) 2019/882***[17] ***eller en specifik social eller ekonomisk situation som sannolikt kommer att göra dessa personer mer sårbara för utnyttjande, såsom personer som lever i extrem fattigdom, etniska minoriteter eller religiösa minoriteter.***

[17] Europaparlamentets och rådets direktiv (EU) 2019/882 av den 17 april 2019 om tillgänglighetskrav för produkter och tjänster (EUT L 151, 7.6.2019, s. 70).

Sådana AI-system kan släppas ut på marknaden, tas i bruk eller användas med ***målet eller verkan att*** väsentligt ***snedvrida*** en persons beteende och på ett sätt som orsakar eller ***rimligt*** sannolikt kommer att orsaka ***betydande*** skada för den personen ***eller en annan person eller grupper av personer, inbegripet skador som kan ackumuleras över tid, och bör därför förbjudas***. Det är kanske inte möjligt att anta att det finns en avsikt att ***snedvrida beteendet***, om snedvridningen beror på faktorer utanför AI-systemet som ligger utanför leverantörens eller ***spridarens*** kontroll***, dvs. faktorer som kanske inte är rimligen förutsebara och därför inte kan begränsas av leverantören eller spridaren av AI-systemet***. ***I vilket fall som helst är det inte nödvändigt att leverantören eller spridaren har för avsikt att orsaka den betydande skadan, förutsatt att sådan skada beror på de manipulativa eller utnyttjande AI-baserade metoderna. Förbuden mot sådana AI-metoder kompletterar bestämmelserna i Europaparlamentets och rådets direktiv 2005/29/EG[18], särskilt att otillbörliga affärsmetoder som leder till ekonomisk eller finansiell skada för konsumenterna är förbjudna under alla omständigheter, oavsett om de har införts genom AI-system eller på annat sätt. Förbuden mot manipulativa och utnyttjande metoder i denna förordning bör inte påverka lagliga metoder i samband med medicinsk behandling, såsom psykologisk behandling av en psykisk sjukdom eller fysisk rehabilitering, när dessa metoder*** utförs i enlighet med ***tillämplig lag och tillämpliga medicinska*** normer***, till exempel de enskilda personernas eller deras ombuds uttryckliga samtycke***. ***Dessutom bör vanliga och legitima affärsmetoder, till exempel på reklamområdet, som är förenliga med tillämplig lagstiftning inte i sig anses utgöra skadliga manipulativa AI-metoder.***

[18] Europaparlamentets och rådets direktiv 2005/29/EG av den 11 maj 2005 om otillbörliga affärsmetoder som tillämpas av näringsidkare gentemot konsumenter på den inre marknaden och om ändring av rådets direktiv 84/450/EEG och Europaparlamentets och rådets direktiv 97/7/EG, 98/27/EG och 2002/65/EG samt Europaparlamentets och rådets förordning (EG) nr 2006/2004 | (direktiv om otillbörliga affärsmetoder) (EUT L 149, 11.6.2005, s. 22).

(30) ***System för biometrisk kategorisering som med utgångspunkt i fysiska personers biometriska uppgifter, såsom en enskild persons ansikte eller fingeravtryck, ska härleda eller dra slutsatser om en persons politiska åsikter, medlemskap i fackförening, religiösa eller filosofiska övertygelse, ras, sexualliv eller sexuella läggning bör förbjudas. Detta förbud omfattar inte laglig märkning, filtrering eller kategorisering av biometriska dataset som förvärvats i enlighet med unionsrätten eller nationell rätt på grundval av biometriska uppgifter, såsom sortering av bilder enligt hår- eller ögonfärg, som till exempel kan användas inom brottsbekämpning.***

(31) AI-system som tillhandahåller ▌ offentliga ***eller privata aktörers*** sociala poängsättning av fysiska personer kan medföra diskriminering och uteslutning av vissa grupper. De kan strida mot rätten till värdighet och icke-diskriminering och värdena jämlikhet och rättvisa. Sådana AI-system utvärderar eller klassificerar ***fysiska personer eller grupper av sådana*** på grundval av ***flera datapunkter relaterade till*** deras sociala beteende i olika sammanhang eller kända***, uttydda*** eller förutsedda personliga egenskaper eller personlighetsegenskaper ***under vissa tidsperioder***. Den sociala poängsättning som erhålls från sådana AI-system kan leda till negativ eller ogynnsam behandling av fysiska personer eller hela grupper av fysiska personer i sociala sammanhang som saknar koppling till det sammanhang där berörda data ursprungligen genererades eller samlades in, eller till en negativ behandling som är oproportionerlig eller omotiverad i förhållande till hur allvarligt deras sociala beteende är. ***AI-system som medför sådana oacceptabla poängsättningsmetoder och som leder till sådana negativa eller ogynnsamma resultat*** bör därför förbjudas. ***Detta förbud bör inte påverka lagliga metoder för bedömning av fysiska personer som utförs för ett specifikt ändamål i enlighet med unionsrätten och nationell rätt.***

(32) Användningen av system för biometrisk fjärridentifiering i realtid av fysiska personer på allmänt tillgängliga platser för brottsbekämpningssyften inkräktar särskilt ***på*** de berörda personernas rättigheter och friheter, i och med att denna användning kan påverka privatlivet för en stor del av befolkningen, kan skapa en känsla av konstant övervakning och indirekt avskräcka från utövande av mötesfrihet och andra grundläggande rättigheter. ***Tekniska brister i AI-system som är avsedda för biometrisk fjärridentifiering av fysiska personer kan leda till snedvridna resultat och medföra diskriminerande effekter. Sådana eventuella snedvridna resultat och diskriminerande effekter är särskilt relevanta när det gäller ålder, etnicitet, ras, kön eller funktionsnedsättning.*** De omedelbara effekterna och de begränsade möjligheterna till ytterligare kontroll eller korrigering när det gäller användningen av sådana system som fungerar i realtid innebär att de medför ökade risker för rättigheterna och friheterna för de personer som berörs av brottsbekämpningen.

(33) Användningen av sådana system för brottsbekämpning bör därför vara förbjuden, utom i de snävt definierade situationer som anges i den uttömmande förteckningen, i de fall då användningen är strikt nödvändig för att uppnå ett väsentligt allmänintresse, vars betydelse är större än riskerna. Dessa situationer inbegriper sökandet efter ***vissa*** brottsoffer, ▌ inklusive försvunna ***personer***, vissa hot mot fysiska personers liv eller fysiska säkerhet eller hot om en terroristattack, och lokalisering ***eller identifiering*** av gärningsmän till eller misstänkta för brott som förtecknas i bilagan till denna förordning, ***om*** dessa brott kan leda till fängelse eller annan frihetsberövande åtgärd för en maxperiod av minst ***fyra*** år i den berörda medlemsstaten, i enlighet med den medlemsstatens lagstiftning. En sådan tröskel för påföljden fängelse eller annan frihetsberövande åtgärd i enlighet med nationell rätt bidrar till att säkerställa att brottet är allvarligt nog för att potentiellt motivera användningen av system för biometrisk fjärridentifiering i realtid.

Vidare grundas ***dessa brott på*** de 32 brott som förtecknas i rådets rambeslut 2002/584/RIF[19], ***med beaktande av att*** vissa av dessa brott i praktiken sannolikt kommer att vara mer relevanta än andra, i och med att det kommer att variera mycket hur nödvändig och proportionerlig användningen av biometrisk fjärridentifiering i realtid kan förutses vara för det praktiska arbetet med lokalisering ***eller identifiering*** av gärningsmän eller misstänkta när det gäller brott som anges i förteckningen, och med beaktande av de sannolika skillnaderna vad gäller allvarlighetsgrad, sannolikhet och omfattning på skadan eller de möjliga negativa konsekvenserna. ***Ett överhängande hot mot en persons liv eller fysiska säkerhet kan också vara följden av en allvarlig driftsstörning vid kritisk infrastruktur enligt definitionen i artikel 2.4 i Europaparlamentets och rådets direktiv (EU) 2022/2557[20], om en driftsstörning vid eller förstörelse av sådan kritisk infrastruktur skulle leda till en omedelbar fara för en persons liv eller fysiska säkerhet, inbegripet genom allvarlig skada på tillhandahållandet av basförnödenheter till befolkningen eller på utövandet av statens kärnfunktion. Dessutom bör denna förordning bevara möjligheten för brottsbekämpande myndigheter, gränskontrollmyndigheter, immigrations- eller asylmyndigheter att utföra identitetskontroller i närvaro av den berörda personen i enlighet med villkoren i unionsrätten och nationell rätt för sådana kontroller. I synnerhet bör brottsbekämpande myndigheter, gränskontrollmyndigheter, immigrationsmyndigheter eller asylmyndigheter kunna använda informationssystem, i enlighet med unionsrätten eller nationell rätt, för att identifiera personer som under en identitetskontroll antingen vägrar att identifieras eller inte kan ange eller bevisa sin identitet, utan att det enligt denna förordning krävs förhandstillstånd. Detta kan till exempel röra sig om en person som är inblandad i ett brott, är ovillig eller på grund av en olycka eller ett medicinskt tillstånd är oförmögen att uppge sin identitet för brottsbekämpande myndigheter.***

---

[19] ***Rådets rambeslut 2002/584/RIF av den 13 juni 2002 om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna (EGT L 190, 18.7.2002, s. 1).***

[20] Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (EUT L 333, 27.12.2022, s. 164).

(34) För att säkerställa att dessa system används på ett ansvarsfullt och proportionerligt sätt är det också viktigt att fastställa att hänsyn bör tas till vissa faktorer i var och en av de snävt definierade situationerna i den uttömmande förteckningen, i synnerhet vad gäller arten av situation som ger upphov till begäran och användningens konsekvenser för alla berörda personers rättigheter och friheter samt de skyddsåtgärder och villkor som föreskrivs i samband med användningen. Användningen av system för biometrisk fjärridentifiering i realtid på allmänt tillgänglig plats för brottsbekämpande ändamål bör ***utnyttjas endast för att bekräfta identiteten av den individ som särskilt avses och bör begränsas till vad som är strikt nödvändigt vad gäller tidsperiod samt geografiskt och personligt tillämpningsområde,*** med särskild hänsyn till bevis eller indikationer vad gäller hoten, offren eller gärningsmännen. ***Användningen av systemet för biometrisk fjärridentifiering i realtid på allmänt tillgänglig plats bör tillåtas endast om den relevanta brottsbekämpande myndigheten har slutfört en konsekvensbedömning avseende grundläggande rättigheter och, om inte annat föreskrivs i denna förordning, har registrerat systemet i den databas som föreskrivs i denna förordning.*** Referensdatabasen över personer bör vara ändamålsenlig för varje användningsfall i var och en av de situationer som anges ovan.

(35) Varje användning av system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpande ändamål bör vara föremål för ett uttryckligt och specifikt tillstånd som lämnas av en oberoende administrativ myndighet ***vars beslut är bindande*** för en medlemsstat. Dessa tillstånd bör i princip erhållas innan ***AI-systemet används för att identifiera en eller flera personer. Undantag från denna regel bör tillåtas*** av hänsyn till vederbörligen motiverade brådskande situationer, främst situationer då behovet av att använda de ifrågavarande systemen är sådant att det i praktiken är objektivt omöjligt att erhålla ett tillstånd innan användningen av AI-systemet inleds. I sådana brådskande situationer bör användningen av AI-systemet begränsas till det absoluta minimum som är nödvändigt och bör omfattas av lämpliga skyddsmekanismer och villkor som fastställs i nationell lagstiftning och som specificeras av den berörda brottsbekämpande myndigheten i samband med varje enskilt fall av brådskande användning. Dessutom bör den brottsbekämpande myndigheten i sådana situationer ***begära ett sådant*** tillstånd ▌ samtidigt som den anger skälen till att den inte har kunnat begära det tidigare***, utan onödigt dröjsmål och senast inom 24 timmar. Om ett sådant tillstånd avslås bör användningen av system för biometrisk identifiering i realtid som är kopplade till det tillståndet stoppas med omedelbar verkan och alla uppgifter som rör sådan användning bör kasseras och raderas. Sådana data omfattar indata som erhållits direkt av ett AI-system i samband med användningen av ett sådant system samt resultat och utdata från den användning som är kopplad till godkännandet. Det bör inte omfatta indata som lagligen förvärvats i enlighet med annan unionslagstiftning eller nationell lagstiftning. Under inga omständigheter bör beslut som har negativa rättsliga följder för en person baseras enbart på grundval av utdata från systemet för biometrisk fjärridentifiering.***

(36) För att kunna utföra sina uppgifter i enlighet med kraven i denna förordning och i nationella regler bör den berörda marknadskontrollmyndigheten och den nationella dataskyddsmyndigheten underrättas om varje användning av systemet för biometrisk identifiering i realtid. De nationella marknadskontrollmyndigheterna och de nationella dataskyddsmyndigheter som har underrättats bör lämna in en årlig rapport till kommissionen om användningen av systemet för biometrisk identifiering i realtid.

(37) Det är också lämpligt att, inom den uttömmande ram som fastställs genom denna förordning, föreskriva att en sådan användning på en medlemsstats territorium i enlighet med denna förordning endast bör vara möjlig i de fall och i den utsträckning som den berörda medlemsstaten har beslutat att uttryckligen föreskriva möjligheten att tillåta sådan användning i sina närmare bestämmelser i nationell lagstiftning. Enligt denna förordning behåller alltså medlemsstaterna sin frihet att inte alls föreskriva någon sådan möjlighet eller att endast föreskriva en sådan möjlighet med avseende på några av de syften som kan motivera användning som tillåten enligt denna förordning. ***Sådana nationella bestämmelser bör anmälas till kommissionen senast 30 dagar efter det att de har antagits.***

(38) Användningen av system för biometrisk fjärridentifiering i realtid av fysiska personer på allmänt tillgängliga platser för brottsbekämpande ändamål involverar med nödvändighet behandling av biometriska uppgifter. Reglerna i denna förordning som med vissa undantag förbjuder sådan användning, och som baseras på artikel 16 i EUF-fördraget, bör tillämpas som *lex specialis* med avseende på de regler om behandling av biometriska uppgifter som anges i artikel 10 i direktiv (EU) 2016/680, och reglerar därmed sådan användning och behandling av berörda biometriska uppgifter på ett uttömmande sätt. Därför bör sådan användning och behandling vara möjlig endast i den utsträckning som den är förenlig med den ram som fastställs i denna förordning, utan att de behöriga myndigheterna har något utrymme, då de agerar för brottsbekämpningsändamål, att utanför den ramen använda sådana system och behandla sådana data i samband med detta av de skäl som förtecknas i artikel 10 i direktiv (EU) 2016/680. I det sammanhanget är denna förordning inte avsedd att tillhandahålla en rättslig grund för behandling av personuppgifter enligt artikel 8 i direktiv (EU) 2016/680. Användningen av system för biometrisk fjärridentifiering i realtid på allmänt tillgänglig plats för andra ändamål än brottsbekämpning, inbegripet av offentliga myndigheter, bör inte omfattas av den särskilda ram för sådan användning för brottsbekämpningsändamål som fastställs i denna förordning. Sådan användning för andra ändamål än brottsbekämpning bör därför inte omfattas av kravet på tillstånd enligt denna förordning och de tillämpliga närmare bestämmelser i nationell lagstiftning som kan ge verkan åt det tillståndet.

(39) Användning av biometriska uppgifter och andra personuppgifter i samband med användningen av AI-system för biometrisk identifiering som inte sker i samband med användning av system för biometrisk fjärridentifiering i realtid på allmänt tillgänglig plats i brottsbekämpningssyfte som regleras av denna förordning ***bör även fortsättningsvis uppfylla alla krav som följer av artikel 10 i direktiv (EU) 2016/680. För andra*** ändamål än brottsbekämpning ***förbjuds*** enligt ▌ artikel 9.1 i förordning (EU) 2016/679 ***och*** artikel 10.1 i förordning (EU) 2018/1725 ***behandling av biometriska uppgifter med förbehåll för begränsade undantag enligt dessa artiklar. Med tillämpning av artikel 9.1 i förordning (EU) 2016/679 har användningen av biometrisk fjärridentifiering för andra ändamål än brottsbekämpning redan förbjudits av nationella dataskyddsmyndigheter.***

(40) I enlighet med artikel 6a i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till EU-fördraget och EUF-fördraget, är Irland inte bundet av bestämmelserna i ***artikel 5.1 c i den mån den gäller för system för biometrisk kategorisering inom polissamarbete och straffrättsligt samarbete***, ***artikel 5.1 e och 5.1 f i den mån den gäller för användning av AI-system som omfattas av den bestämmelsen, artikel*** 5***.3-5.8 samt artikel 26.10*** i den här förordningen som antagits på grundval av artikel 16 i EUF-fördraget och som avser medlemsstaternas behandling av personuppgifter när de bedriver verksamhet som omfattas av avdelning V kapitel 4 eller 5 ii avdelning V tredje delen av EUF-fördraget i det fall då Irland inte är bundet av bestämmelserna om formerna för straffrättsligt samarbete eller polissamarbete inom ramen för vilka de bestämmelser måste iakttas som fastställs på grundval av artikel 16 i EUF-fördraget.

(41) I enlighet med artiklarna 2 och 2a i protokoll nr 22 om Danmarks ställning, fogat till EU-fördraget och EUF-fördraget, är Danmark inte bundet av reglerna i ***artikel 5.1 c i den mån den gäller användning av system för biometrisk kategorisering inom polissamarbete och straffrättsligt samarbete, artikel 5.1 e, 5.1 f i den mån den gäller för användning av AI-system som omfattas av den bestämmelsen***, artikel 5***.3-5.8 samt artikel 26.10*** i den här förordningen som antagits på grundval av artikel 16 i EUF-fördraget, eller tillämpningen av dessa, som avser medlemsstaternas behandling av personuppgifter när dessa utövar verksamhet som omfattas av tillämpningsområdet för kapitel 4 eller 5 i avdelning V i tredje delen av EUF-fördraget.

(42) I enlighet med oskuldspresumtionen bör fysiska personer i unionen alltid bedömas utifrån sitt faktiska beteende. Fysiska personer bör aldrig bedömas på grundval av genom AI förutsett beteende enbart grundat på deras profilering, personlighetsdrag eller egenskaper, såsom nationalitet, födelseort, bostadsort, antal barn, skuldnivå eller typ av bil, utan rimlig misstanke om att personen är inblandad i en brottslig verksamhet på grundval av objektiva, kontrollerbara fakta och utan mänsklig bedömning av detta. Därför bör riskbedömningar som genomförs med avseende på fysiska personer för att bedöma risken för att de begår brott eller för att förutsäga förekomsten av ett faktiskt eller potentiellt brott enbart på grundval av deras profilering eller en bedömning av deras personlighetsdrag och egenskaper förbjudas. I vilket fall som helst avser eller berör förbudet inte riskanalyser som inte baseras på profilering av enskilda personer eller på enskilda personers personlighetsdrag och egenskaper, såsom AI-system som använder riskanalyser för att bedöma risken för ekonomiska bedrägerier från företags sida på grundval av misstänkta transaktioner eller riskanalysverktyg för förutsägelser om sannolikheten för narkotikas eller olagliga varors läge från tullmyndigheternas sida, till exempel på grundval av kända smugglingsvägar.

(43) Utsläppande på marknaden, ibruktagande för detta specifika ändamål eller användning av AI-system som skapar eller utvidgar databaser för ansiktsigenkänning genom oriktad skrapning av ansiktsbilder från internet eller övervakningskameror bör förbjudas, eftersom metoden ökar känslan av att det förekommer massövervakning och kan leda till grova kränkningar av grundläggande rättigheter, inbegripet rätten till integritet.

(44) Det råder allvarlig oro över den vetenskapliga grunden för AI-system som syftar till att identifiera eller uttyda känslor, särskilt som uttryck för känslor varierar avsevärt mellan olika kulturer och situationer och till och med hos en och samma individ. Några av de största bristerna i sådana system är begränsad tillförlitlighet, brist på specificitet och begränsad generaliserbarhet. AI-system som identifierar eller uttyder fysiska personers känslor eller avsikter på grundval av deras biometriska uppgifter kan därför leda till diskriminerande resultat och kan inkräkta på de berörda personernas rättigheter och friheter. Med tanke på maktobalansen i fråga om arbete eller utbildning, i kombination med dessa systems inkräktande karaktär, kan sådana system leda till skadlig eller ogynnsam behandling av vissa fysiska personer eller hela grupper av fysiska personer. Därför bör utsläppande på marknaden, ibruktagande eller användning av AI-system som är avsedda att användas för att upptäcka känslomässiga förhållanden hos enskilda personer i situationer som rör arbetsplats och utbildning förbjudas. Förbudet bör inte omfatta AI-system som släpps ut på marknaden uteslutande av medicinska skäl eller säkerhetsskäl, såsom system som är avsedda för terapeutisk användning.

(45) Metoder som är förbjudna enligt unionsrätten, inbegripet dataskyddslagstiftning, lagstiftning om icke-diskriminering, konsumentskyddslagstiftning och konkurrensrätt, bör inte påverkas av denna förordning.

(46) AI-system med hög risk bör endast släppas ut på unionsmarknaden ***eller tas i bruk*** om de uppfyller vissa obligatoriska krav. Dessa krav bör säkerställa att AI-system med hög risk vilka finns tillgängliga i unionen eller vars utdata på annat sätt används i unionen inte utgör någon oacceptabel risk för viktiga allmänna intressen för unionen som erkänns och skyddas av unionsrätten. ***Baserat på den nya lagstiftningsramen, som klargörs i kommissionens meddelande 2022 års blåbok om genomförandet av EU:s produktbestämmelser[21], är den allmänna regeln att sådan unionsharmoniseringslagstiftning som Europaparlamentets och rådets förordningar (EU) 2017/745[22] och (EU) 2017/746[23] samt Europaparlamentets och rådets direktiv 2006/42/EG[24] kan äga tillämpning med avseende på en produkt, eftersom tillhandahållandet eller ibruktagandet endast kan ske när produkten överensstämmer med all tillämplig unionsharmoniseringslagstiftning. För att säkerställa konsekvens och undvika en onödig administrativ börda eller onödiga kostnader bör leverantörer av en produkt som innehåller ett eller flera AI-system med hög risk som omfattas av kraven i denna förordning eller i unionens harmoniseringslagstiftning i förteckningen i en bilaga till denna förordning vara flexibla när det gäller operativa beslut om hur man på bästa sätt ska säkerställa att en produkt som innehåller ett eller flera AI-system uppfyller alla tillämpliga krav i unionens harmoniseringslagstiftning på ett optimalt sätt.*** AI-system som identifieras som hög risk bör begränsas till sådana som har en betydande skadlig inverkan på hälsa, säkerhet och grundläggande rättigheter för personer i unionen och denna avgränsning minimerar de potentiella begränsningarna av den internationella handeln.

---

21 ***EUT C 247, 29.6.2022, s. 1.***

22 Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, om ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG (EUT L 117, 5.5.2017, s. 1).

23 Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för in vitro-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU (EUT L 117, 5.5.2017, s. 176).

24 Europaparlamentets och rådets direktiv 2006/42/EG av den 17 maj 2006 om maskiner och om ändring av direktiv 95/16/EG (EUT L 157, 9.6.2006, s. 24).

(47) AI-system ***kan*** producera negativa ***effekter*** för personers hälsa och säkerhet, i synnerhet när sådana system fungerar som ***säkerhet***skomponenter. I enlighet med syftena för unionens harmoniseringslagstiftning, som är att främja den fria rörligheten för produkter på den inre marknaden och säkerställa att endast säkra produkter som uppfyller kraven släpps ut på marknaden, är det viktigt att de säkerhetsrisker som kan genereras av produkten som helhet på grund av dess digitala komponenter, inklusive AI-system, förhindras och begränsas. Robotar som blir allt mer autonoma, oavsett om det är i samband med tillverkning eller personlig assistans och vård, bör också kunna arbeta säkert och utföra sina funktioner i komplexa miljöer. Inom vårdsektorn, där liv och hälsa i särskilt hög grad kan påverkas, bör de allt mer sofistikerade diagnossystemen och systemen som stöder mänskliga beslut vara tillförlitliga och noggranna. ▌

(48) Omfattningen av de negativa effekter som AI-systemet har på de grundläggande rättigheter som skyddas av stadgan har särskilt stor betydelse när ett AI-system klassificeras som hög risk Dessa rättigheter innefattar rätten till människans värdighet, respekt för privatlivet och familjelivet, skydd av personuppgifter, yttrandefrihet och informationsfrihet, mötesfrihet och organisationsfrihet samt icke-diskriminering, rätten till utbildning, konsumentskydd, arbetstagares rättigheter, rättigheter för personer med funktionsnedsättning, jämställdhet, immateriella rättigheter, rätten till ett effektivt rättsmedel och till en opartisk domstol, rätten till försvar och oskuldspresumtion samt rätten till god förvaltning. Vid sidan av dessa rättigheter är det viktigt att lyfta fram den omständigheten att barn har särskilda rättigheter i enlighet med artikel 24 i stadgan och Förenta nationernas konvention om barnets rättigheter (som vidareutvecklas i konventionens allmänna kommentar nr 25 vad gäller den digitala miljön), som båda kräver att barns utsatthet beaktas och att de ges ett sådant skydd och sådan omsorg som krävs för deras välbefinnande. Även den grundläggande rättigheten till en hög nivå av miljöskydd, som också ingår i stadgan och genomförs i unionspolitik, bör beaktas vid bedömningen av allvarlighetsgraden i den skada som ett AI-system kan orsaka, inbegripet vad gäller människors hälsa och säkerhet.

(49) När det gäller AI-system med hög risk som är säkerhetskomponenter i produkter eller system, eller som i sig själva utgör produkter eller system som omfattas av Europaparlamentets och rådets förordning (EG) nr 300/2008[25], Europaparlamentets och rådets förordning (EU) nr 167/2013[26], Europaparlamentets och rådets förordning (EU) nr 168/2013[27], Europaparlamentets och rådets direktiv 2014/90/EU[28], Europaparlamentets och rådets direktiv (EU) 2016/797[29], Europaparlamentets och rådets förordning (EU) 2018/858[30],

[25] Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002 (EUT L 97, 9.4.2008, s. 72).

[26] Europaparlamentets och rådets förordning (EU) nr 167/2013 av den 5 februari 2013 om godkännande och marknadstillsyn av jordbruks- och skogsbruksfordon (EUT L 60, 2.3.2013, s. 1).

[27] Europaparlamentets och rådets förordning (EU) nr 168/2013 av den 15 januari 2013 om godkännande av och marknadstillsyn för två- och trehjuliga fordon och fyrhjulingar (EUT L 60, 2.3.2013, s. 52).

[28] Europaparlamentets och rådets direktiv 2014/90/EU av den 23 juli 2014 om marin utrustning och om upphävande av rådets direktiv 96/98/EG (EUT L 257, 28.8.2014, s. 146).

[29] Europaparlamentets och rådets direktiv (EU) 2016/797 av den 11 maj 2016 om driftskompatibiliteten hos järnvägssystemet inom Europeiska unionen (EUT L 138, 26.5.2016, s. 44).

[30] Europaparlamentets och rådets förordning (EU) 2018/858 av den 30 maj 2018 om godkännande av och marknadskontroll över motorfordon och släpfordon till dessa fordon samt av system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, om ändring av förordningarna (EG) nr 715/2007 och (EG) nr 595/2009 samt om upphävande av direktiv 2007/46/EG (EUT L 151, 14.6.2018, s. 1).

Europaparlamentets och rådets förordning (EU) 2018/1139[31] och Europaparlamentets och rådets förordning (EU) 2019/2144[32], är det lämpligt att ändra dessa akter för att säkerställa att kommissionen, på grundval av de tekniska och regleringsmässiga särdragen för varje sektor och utan att inkräkta på befintliga mekanismer för styrelseformer, för kontroll av överensstämmelse och för kontroll av efterlevnad och myndigheter som inrättats inom ramen för dessa, beaktar de obligatoriska krav för AI-system med hög risk som fastställs i denna förordning när de antar relevanta delegerade akter eller genomförandeakter på grundval av dessa akter.

[31] Europaparlamentets och rådets förordning (EU) 2018/1139 av den 4 juli 2018 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 2111/2005, (EG) nr 1008/2008, (EU) nr 996/2010, (EU) nr 376/2014 och direktiv 2014/30/EU och 2014/53/EU, samt om upphävande av Europaparlamentets och rådets förordningar (EG) nr 552/2004 och (EG) nr 216/2008 och rådets förordning (EEG) nr 3922/91, (EUT L 212, 22.8.2018, s. 1).

[32] Europaparlamentets och rådets förordning (EU) 2019/2144 av den 27 november 2019 om krav för typgodkännande av motorfordon och deras släpvagnar samt de system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, med avseende på deras allmänna säkerhet och skydd för personer i fordonet och oskyddade trafikanter, om ändring av Europaparlamentets och rådets förordning (EU) 2018/858 och om upphävande av Europaparlamentets och rådets förordningar (EG) nr 78/2009, (EG) nr 79/2009 och (EG) nr 661/2009 samt kommissionens förordningar (EG) nr 631/2009, (EU) nr 406/2010, (EU) nr 672/2010, (EU) nr 1003/2010, (EU) nr 1005/2010, (EU) nr 1008/2010, (EU) nr 1009/2010, (EU) nr 19/2011, (EU) nr 109/2011, (EU) nr 458/2011, (EU) nr 65/2012, (EU) nr 130/2012, (EU) nr 347/2012, (EU) nr 351/2012, (EU) nr 1230/2012 och (EU) 2015/166 (EUT L 325, 16.12.2019, s. 1).

(50) När det gäller AI-system som är säkerhetskomponenter i produkter, eller som i sig själva utgör produkter, vilka omfattas av viss unionslagstiftning om harmonisering, är det lämpligt att klassificera dessa som hög risk inom ramen för denna förordning om den berörda produkten genomgår förfarandet för bedömning av överensstämmelse hos ett tredjepartsorgan för bedömning av överensstämmelse i enlighet med den relevanta unionslagstiftningen om harmonisering. Det handlar närmare bestämt om sådana produkter som maskiner, leksaker, hissar, utrustning och skyddssystem avsedda för användning i potentiellt explosionsfarliga omgivningar, radioutrustning, tryckutrustning, utrustning för fritidsfartyg, linbaneanläggningar, anordningar för förbränning av gasformiga bränslen, medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik.

(51) En klassificering av ett AI-system som hög risk i enlighet med denna förordning bör inte nödvändigtvis innebära att den produkt vars säkerhetskomponent utgörs av AI-systemet, eller AI-systemet i sig självt som produkt, anses utgöra ett system med hög risk enligt de kriterier som fastställs i den relevanta unionslagstiftning om harmonisering som är tillämplig på produkten. Detta gäller i synnerhet för förordning (EU) 2017/745 och (EU) 2017/746, i vilka tredjepartsbedömning av överensstämmelse föreskrivs för produkter med medelhög risk och hög risk.

(52) När det gäller fristående AI-system, det vill säga andra AI-system med hög risk än sådana som utgör säkerhetskomponenter, eller AI-system med hög risk som i sig själva utgör produkter, är det lämpligt att klassificera dem som hög risk om de i ljuset av sitt avsedda ändamål utgör en hög risk för skada på personers hälsa och säkerhet eller grundläggande rättigheter, med beaktande både den möjliga skadans allvarlighetsgrad och sannolikheten för att den ska uppstå, och de används på ett antal specifikt fördefinierade områden som anges i denna förordning. Identifieringen av sådana system baseras på samma metoder och kriterier som även är avsedda att användas för framtida ändringar av förteckningen över AI-system med hög risk ***som kommissionen bör ges befogenhet att anta, genom delegerade akter, för att ta hänsyn till den snabba tekniska utvecklingen samt potentiella förändringar i användningen av AI-system.***

(53) Det är också viktigt att klargöra att det kan finnas särskilda fall där AI-system som avser fördefinierade områden som specificeras i denna förordning inte leder till en betydande risk för skada för de rättsliga intressen som skyddas inom dessa områden, eftersom de inte väsentligt påverkar beslutsfattandet eller inte skadar dessa intressen väsentligt. Vid tillämpningen av denna förordning bör ett AI-system som inte väsentligt påverkar resultatet av beslutsfattandet förstås som ett AI-system som inte påverkar innehållet, och därmed resultatet, av beslutsfattandet, oavsett om det är mänskligt eller automatiserat. Ett AI-system som inte väsentligt påverkar resultatet av beslutsfattandet kan omfatta situationer där ett eller flera av nedanstående villkor är uppfyllda. Det första sådana villkoret bör vara att AI-systemet är avsett att utföra en snäv processuell uppgift, såsom ett AI-system som omvandlar ostrukturerade data till strukturerade data, ett AI-system som klassificerar inkommande handlingar i kategorier eller ett AI-system som används för att upptäcka dubbletter bland ett stort antal applikationer. Dessa uppgifter är av så snäv och begränsad art att de endast medför begränsade risker som inte ökar genom användning i ett sammanhang som förtecknas som hög risk i en bilaga till denna förordning. Det andra villkoret bör vara att den uppgift som utförs av AI-systemet är avsedd att förbättra resultatet av tidigare fullbordad mänsklig verksamhet som kan vara relevant för den förteckningen. Med tanke på dessa egenskaper tillhandahåller AI-systemet endast ett extra skikt till mänsklig verksamhet och innebär följaktligen lägre risk. Detta villkor skulle till exempel tillämpas på AI-system som är avsedda att förbättra det språk som används i tidigare utarbetade dokument, till exempel när det gäller yrkesmässig ton eller akademisk språkstil eller genom att anpassa texten till ett visst varumärkesbudskap.

Det tredje villkoret bör vara att AI-systemet är avsett att upptäcka beslutsmönster eller avvikelser från tidigare beslutsmönster. Risken skulle minska eftersom användningen av AI-systemet följer en tidigare slutförd mänsklig bedömning som den inte avser ersätta eller påverka utan ordentlig mänsklig granskning. Sådana AI-system omfattar till exempel system som, med tanke på en viss lärares betygsättningsmönster, kan användas för att i efterhand kontrollera om läraren har avvikit från betygsättningsmönstret för att på så sätt uppmärksamma potentiella inkonsekvenser eller avvikelser. Det fjärde villkoret bör vara att AI-systemet är avsett att utföra en uppgift som endast är förberedande för en bedömning som är relevant för de AI-system som förtecknas i en bilaga till denna förordning, så att den möjliga effekten av systemets utdata blir mycket låg när det gäller att utgöra en risk för den bedömning som ska följa. Detta villkor omfattar bland annat smarta lösningar för ärendehandläggning som omfattar olika funktioner såsom indexering, sökning, text- och talbehandling eller länkning av data till andra datakällor, eller AI-system som används för översättning av ursprungliga dokument. Under alla omständigheter bör dessa AI-system med hög risk anses utgöra en betydande risk för skada på fysiska personers hälsa, säkerhet eller grundläggande rättigheter om AI-systemet innebär profilering i den mening som avses i artikel 4.4 i förordning (EU) 2016/679 eller artikel 3.4 i direktiv (EU) 2016/680 eller artikel 3.5 i förordning (EU) 2018/1725. För att säkerställa spårbarhet och transparens bör en leverantör som anser att ett AI-system inte är förenat med hög risk på grundval av dessa villkor upprätta dokumentation om bedömningen innan systemet släpps ut på marknaden eller tas i bruk och bör på begäran tillhandahålla denna dokumentation till de nationella behöriga myndigheterna. En sådan leverantör bör vara skyldig att registrera systemet i den EU-databas som inrättas enligt denna förordning. I syfte att ge ytterligare vägledning för det praktiska genomförandet av de villkor enligt vilka AI-system med hög risk som förtecknas i bilagan undantagsvis inte är förenade med hög risk bör kommissionen, efter samråd med nämnden, ge riktlinjer som specificerar detta praktiska genomförande, kompletterat med en omfattande förteckning över praktiska exempel på användning av AI-system med och utan hög risk.

▌

(54) Eftersom biometriska uppgifter utgör en särskild kategori av känsliga personuppgifter är det lämpligt att klassificera flera kritiska användningsfall av biometriska system som hög risk, i den mån användningen av dem är tillåten enligt relevant unionsrätt och nationell rätt. Tekniska brister i AI-system som är avsedda för biometrisk fjärridentifiering av fysiska personer kan leda till snedvridna resultat och medföra diskriminerande effekter. Risken för sådana snedvridna resultat och diskriminerande effekter är särskilt relevant när det gäller ålder, etnicitet, ras, kön eller funktionsnedsättning. System för biometrisk fjärridentifiering bör därför klassificeras som system med hög risk med tanke på de risker de medför. En sådan klassificering utesluter AI-system som är avsedda att användas för biometrisk verifiering, inbegripet autentisering, vars enda syfte är att bekräfta att en specifik fysisk person är den som vederbörande utger sig för att vara och för att bekräfta identiteten för en fysisk person med det enda syftet att få åtkomst till en tjänst, låsa upp en enhet eller ha säker tillgång till lokaler. Dessutom bör AI-system som är avsedda att användas för biometrisk kategorisering enligt känsliga attribut eller egenskaper som skyddas enligt artikel 9.1 i förordning (EU) 2016/679 på grundval av biometriska uppgifter, i den mån dessa inte är förbjudna enligt denna förordning, och system för känsloigenkänning som inte är förbjudna enligt denna förordning, klassificeras som hög risk. Biometriska system som är avsedda att användas enbart för att möjliggöra cybersäkerhet och åtgärder för skydd av personuppgifter bör inte betraktas som system med hög risk.

(55) När det gäller förvaltning och drift av kritisk infrastruktur är det lämpligt att som hög risk klassificera AI-system avsedda att användas som säkerhetskomponenter i förvaltningen och driften av ***kritisk digital infrastruktur enligt förteckningen i bilaga I punkt 8 till direktiv (EU) 2022/2557***, vägtrafik och tillhandahållandet av vatten, gas, uppvärmning och el, eftersom funktionsavbrott eller funktionsstörning i sådana system kan medföra risk för personers liv och hälsa i stor skala och leda till märkbara störningar av det normala bedrivandet av social och ekonomisk verksamhet. ***Säkerhetskomponenter i kritisk infrastruktur, inbegripet kritisk digital infrastruktur, är system som används för att direkt skydda kritisk infrastrukturs fysiska integritet eller människors hälsa och säkerhet och egendom, men som inte är nödvändiga för att systemet ska fungera. Funktionsavbrott eller funktionsstörning i sådana komponenter kan direkt leda till risker för den kritiska infrastrukturens fysiska integritet och därmed till risker för människors hälsa och säkerhet och egendom. Komponenter som är avsedda att användas enbart för cybersäkerhetsändamål bör inte betraktas som säkerhetskomponenter. Exempel på säkerhetskomponenter i sådan kritisk infrastruktur kan omfatta system för övervakning av vattentryck eller styrsystem för brandlarm vid centrum för molntjänster.***

(56) ***Införandet av AI-system inom utbildningen är viktigt för att främja digital utbildning av hög kvalitet och göra det möjligt för alla studerande och lärare att förvärva och dela de digitala färdigheter och kompetenser som krävs, inbegripet mediekunnighet, och kritiskt tänkande, för att aktivt delta i ekonomin, samhället och i demokratiska processer. AI-*** system som används för yrkesutbildning eller annan utbildning, i synnerhet när det gäller fastställandet av personers tillgång till eller ***antagning till*** institutioner för yrkesutbildning eller annan utbildning eller ***program på alla nivåer, eller för utvärdering av*** personers ***läranderesultat***, ***för bedömning av en persons lämpliga utbildningsnivå och för väsentlig påverkan av den utbildningsnivå som personer kommer att få eller kommer kunna få tillgång till, eller för övervakning och upptäckt av förbjudet beteende bland studerande under provtillfällen,*** bör ***klassificeras som AI-system med hög risk*** eftersom de kan avgöra en persons utbildningsväg och yrkeskarriär och därmed påverka en persons försörjningsmöjligheter. När sådana system utformas och används på otillbörligt sätt ***kan de vara särskilt inkräktande och*** kan innebära en kränkning av rätten till yrkesutbildning och annan utbildning liksom rätten att inte utsättas för diskriminering eller för en fortsättning på historiska diskrimineringsmönster ***mot till exempel kvinnor, vissa åldersgrupper, personer med funktionsnedsättning eller personer av vissa etniska ursprung eller av viss sexuell läggning.***

(57) AI-system som används i utbildning, arbetsledning och tillgång till egenföretagande, i synnerhet när det gäller rekrytering eller urval av personer, för beslutsfattande ***som påverkar villkoren för arbetsrelaterad*** befordran eller uppsägning ***av arbetsrelaterade avtalsförhållanden för fördelning av uppgifter på grundval av individuellt beteende eller personlighetsdrag och egenskaper och för*** övervakning eller utvärdering av personer i arbetsrelaterade avtalsförhållanden, bör också klassificeras som hög risk, eftersom dessa system märkbart kan påverka framtida karriärutsikter och försörjning för dessa personer ***samt arbetstagarnas rättigheter.*** Relevanta arbetsrelaterade avtalsförhållanden bör på ett ***meningsfullt sätt*** innefatta arbetstagare och personer som tillhandahåller tjänster via plattformar enligt kommissionens arbetsprogram för 2021. ▌ Under hela rekryteringsförfarandet och vid utvärdering, befordran eller bibehållande av personer i arbetsrelaterade avtalsförhållanden, kan sådana system reproducera historiska mönster av diskriminering, exempelvis mot kvinnor, vissa åldersgrupper, personer med funktionsnedsättning eller mot personer på grund av ras, etniskt ursprung eller sexuell läggning. AI-system som används för att övervaka sådana personers prestation och beteende kan också ***undergräva*** deras ***grundläggande*** rätt till dataskydd och personlig integritet.

(58) Ett annat område där användningen av AI-system förtjänar särskild vaksamhet är när det gäller tillgång till och åtnjutande av vissa väsentliga privata och offentliga tjänster och förmåner som är nödvändiga för att människor fullt ut ska kunna delta i samhället eller förbättra sin levnadsstandard. I synnerhet ▌ är fysiska personer ***som ansöker om eller får viktiga offentliga bidragsförmåner och tjänster från offentliga myndigheter, nämligen hälso- och sjukvård***stjänster, ***sociala trygghetsförmåner, sociala*** tjänster ***som tillhandahåller skydd i fall som moderskap, sjukdom, arbetsolyckor, vårdbehov eller ålderdom och arbetslöshet samt socialbidrag och bostad***sbidrag, vanligtvis beroende av dessa förmåner och tjänster och befinner sig i en utsatt situation i förhållande till de ansvariga myndigheterna. Om AI-system används för att avgöra om sådana förmåner och tjänster ska ***beviljas***, vägras, minskas, upphävas eller återkallas av myndigheterna, ***inbegripet huruvida mottagarna är legitimt berättigade till sådana förmåner eller tjänster,*** kan ***dessa system*** ha en betydande inverkan på personers försörjning och kan inkräkta på deras grundläggande rättigheter, såsom rätten till socialt skydd, icke-diskriminering, mänsklig värdighet eller effektivt rättsmedel ***och*** bör där klassificeras som hög risk. Denna förordning bör dock inte hämma utvecklingen och användningen av innovativa metoder inom offentlig förvaltning, som kan gagnas av en bredare användning av säkra AI-system som uppfyller kraven, förutsatt att dessa system inte medför hög risk för juridiska och fysiska personer.

Dessutom bör AI-system som används för att utvärdera fysiska personers kreditomdöme eller kreditvärdighet klassificeras som AI-system med hög risk, eftersom de avgör de berörda personernas tillgång till ekonomiska resurser eller väsentliga tjänster som bostad, el och telekommunikationstjänster. AI-system som används för dessa ändamål kan medföra diskriminering av personer eller grupper och kan reproducera sådana historiska diskrimineringsmönster som det som baseras på rasmässigt eller etniskt ursprung, kön, funktionsnedsättning, ålder eller sexuell läggning, eller skapa nya former av diskrimineringseffekter. AI-system som föreskrivs i unionsrätten i syfte att upptäcka bedrägerier i samband med tillhandahållande av finansiella tjänster och för tillsynsändamål för att beräkna kreditinstituts och försäkringsföretags kapitalkrav bör dock inte betraktas som högrisksystem enligt denna förordning. Vidare kan AI-system som är avsedda att användas för riskbedömning och prissättning när det gäller fysiska personer av sjuk- och livförsäkring också ha en betydande inverkan på människors försörjningsmöjligheter och kan, om de inte utformas, utvecklas och används på rätt sätt, inkräkta på deras grundläggande rättigheter och leda till allvarliga konsekvenser för människors liv och hälsa, inbegripet ekonomisk utestängning och diskriminering. Slutligen bör även AI-system som används för att ***utvärdera och klassificera nödsamtal från fysiska personer eller för att*** sända ut eller fastställa prioriteringsordning för utsändning av larmtjänster***, inbegripet av polis, brandkår och sjukvård,*** s***amt av patientsorteringssystem för akutsjukvård*** klassificeras som hög risk, eftersom dessa system fattar beslut i situationer som är mycket kritiska för personers liv, hälsa och egendom.

(59) ***Med tanke på*** de brottsbekämpande myndigheternas ***roll och ansvar*** kännetecknas deras åtgärder, när de omfattar vissa typer av användning av AI-system, av en betydande grad av maktobalans och kan leda till övervakning, gripande eller frihetsberövande av en fysisk person, liksom annan negativ inverkan på grundläggande rättigheter som garanteras i stadgan. De kan – i synnerhet om AI-systemen inte tränats med data av hög kvalitet, inte uppfyller lämpliga krav i fråga om ***prestanda***, noggrannhet eller robusthet, eller inte utformats och testats tillräckligt innan de släpps ut på marknaden eller på annat sätt tas i bruk – peka ut människor på ett diskriminerande eller på ett annat oriktigt eller orättvist sätt. Dessutom kan utövandet av viktiga förfarandemässiga grundläggande rättigheter, såsom rätten till effektivt rättsmedel och till en opartisk domstol samt rätten till försvar och presumtion för oskuld, hämmas, i synnerhet i de fall då AI-systemen inte är tillräckligt transparenta, förklarade och dokumenterade. Det är därför lämpligt att, ***i den mån deras användning är tillåten enligt relevant unionsrätt och nationell rätt***, som hög risk klassificera ett antal AI-system som är avsedda att användas i brottsbekämpningssammanhang där det är särskilt viktigt med noggrannhet, tillförlitlighet och transparens för att undvika negativa effekter, upprätthålla allmänhetens förtroende och säkerställa ansvarsskyldighet och effektiv rättslig prövning.

Mot bakgrund av åtgärdernas art och relaterade risker bör dessa AI-system med hög risk i synnerhet inbegripa AI-system avsedda att användas av ***eller på uppdrag av*** brottsbekämpande myndigheter eller ***av unionens organ, kontor eller byråer till stöd för brottsbekämpande myndigheter vid bedömning av risken för att en*** fysisk person ***ska falla offer för brott, som lögndetektorer och liknande verktyg,*** för utvärdering av bevisens tillförlitlighet ***i samband med utredning eller lagföring av*** brott, ***och, i den mån det inte är förbjudet enligt denna förordning, för bedömning av risken för att en fysisk person begår brott eller återfaller i brott inte enbart på grundval av*** profilering av fysiska personer ***eller en bedömning av*** personlighetsdrag och egenskaper eller tidigare brottsligt beteende hos fysiska personer eller grupper, för profilering i samband med upptäckt, utredning eller lagföring av brott ▌. AI-system som är specifikt avsedda att användas av skattemyndigheter och tullmyndigheter för administrativa förfaranden ***samt av finansunderrättelseenheter som utför administrativa uppgifter för analys av information enligt unionsrätt på området penningtvätt*** bör inte ***klassificeras som*** AI-system med hög risk som används av brottsbekämpande myndigheter i syfte att förebygga, förhindra, avslöja, utreda eller lagföra brott ▌. ***Användningen av AI-verktyg inom brottsbekämpning och av myndigheter bör inte bli en faktor som bidrar till ojämlikhet, sociala klyftor eller utestängning. Den inverkan som användningen av AI-verktyg har på misstänktas rätt till försvar bör inte ignoreras, särskilt svårigheten att få meningsfull information om hur dessa system fungerar och den därav följande svårigheten att överklaga resultaten i domstol, särskilt för fysiska personer som är under utredning.***

(60) AI-system som används i samband med migration, asyl och gränskontrollförvaltning påverkar människor som ofta är i en särskilt utsatt situation och som är beroende av resultatet av de behöriga offentliga myndigheternas åtgärder. Det är därmed särskilt viktigt att de AI-system som används i dessa sammanhang är tillförlitliga, icke-diskriminerande och transparenta, för att garantera iakttagandet av de påverkade personernas grundläggande rättigheter, särskilt deras rätt till fri rörlighet, icke-diskriminering, skydd av privatliv och personuppgifter, internationellt skydd och god förvaltning. ***I den mån deras användning är tillåten enligt relevant unionsrätt och nationell rätt*** är det därför lämpligt att som AI-system med hög risk klassificera AI-system som är avsedda att användas av ***eller på uppdrag av*** de behöriga offentliga myndigheter ***eller av unionens institutioner, organ, kontor eller byråer***, som anförtrotts uppgifter på områdena migration, asyl och gränskontrollförvaltning, såsom lögndetektorer och liknande verktyg, för bedömning av vissa risker som utgörs av fysiska personer som reser in till en medlemsstats territorium eller som ansöker om visering eller asyl, för att bistå behöriga offentliga myndigheter i granskningen, ***inbegripet den relaterade bedömningen av bevisens tillförlitlighet,*** av ansökningar om asyl, visering och uppehållstillstånd och därmed förbundna klagomål med avseende på syftet att fastställa om den ansökande fysiska personen uppfyller kraven för denna status, ***i syfte att upptäcka, känna igen eller identifiera fysiska personer i samband med migration, asyl och gränskontrollförvaltning, med undantag för kontroll av resehandlingar.***

AI-system på området migration, asyl och gränskontrollförvaltning vilka omfattas av denna förordning bör uppfylla de relevanta förfarandemässiga krav som fastställs i Europaparlamentets och rådets förordning (EG) 810/2009[33], Europaparlamentets och rådets direktiv 2013/32/EU[34] och annan relevant unionsrätt. ***AI-system som används i samband med migration, asyl och gränskontrollförvaltning bör under inga omständigheter användas av medlemsstater eller unionens institutioner, organ, kontor eller byråer som ett medel för att kringgå sina internationella skyldigheter enligt FN-konventionen om flyktingars rättsliga ställning, som undertecknades i Genève den 28 juli 1951 i dess ändrade lydelse genom protokollet av den 31 januari 1967. De bör inte heller användas för att på något sätt bryta mot principen om non-refoulement eller neka säkra och effektiva lagliga vägar in på unionens territorium, inbegripet rätten till internationellt skydd.***

[33] ▌Europaparlamentets och rådets förordning (EG) nr 810/2009 av den 13 juli 2009 om införande av en gemenskapskodex om viseringar (viseringskodex) (EUT L 243, 15.9.2009, s. 1).

[34] ▌Europaparlamentets och rådets direktiv 2013/32/EU av den 26 juni 2013 om gemensamma förfaranden för att bevilja och återkalla internationellt skydd (EUT L 180, 29.6.2013, s. 60).

(61) Vissa AI-system som är avsedda för rättsskipning och demokratiska processer bör klassificeras som hög risk, mot bakgrund av deras potentiellt betydande inverkan på demokrati, rättsstatsprincipen, individuella friheter och rätten till effektivt rättsmedel och till en opartisk domstol. För att motverka riskerna för potentiella snedvridningar och fel och bristande insyn är det i synnerhet lämpligt att som AI-system med hög risk klassificera sådana AI-system som är avsedda att ***användas av en rättslig myndighet eller på dess vägnar för att*** hjälpa de rättsliga myndigheterna att efterforska och tolka fakta och lagstiftning och att tillämpa denna lagstiftning på en konkret uppsättning fakta. ***AI-system som är avsedda att användas av organ för alternativ tvistlösning för dessa ändamål bör också anses vara förenade med hög risk när resultaten av förfarandena för alternativ tvistlösning har rättsverkan för parterna. Användningen av AI-verktyg kan stödja domarnas beslutanderätt eller rättsväsendets oberoende men bör inte ersätta det: det slutliga beslutsfattandet måste förbli en människodriven verksamhet. Klassificeringen av AI-system som högrisksystem*** bör dock inte omfatta AI-system som är avsedda för rent administrativa stödfunktioner som inte påverkar den faktiska rättskipningen i enskilda fall, exempelvis anonymisering eller pseudonymisering av rättsliga beslut, handlingar eller data, kommunikation mellan anställda, administrativa uppgifter ▌.

(62) Utan att det påverkar de regler som föreskrivs i Europaparlamentets och rådets förordning (EU) 2024/ ...[35+] och för att hantera riskerna för otillbörlig extern inblandning i rösträtten enligt artikel 39 i stadgan och negativa följder för demokrati och rättsstatsprincipen bör AI-system som är avsedda att användas för att påverka resultatet av ett val eller en folkomröstning eller fysiska personers röstbeteende vid val eller folkomröstningar klassificeras som AI-system med hög risk, med undantag för AI-system vars utdata fysiska personer inte är direkt exponerade för, såsom verktyg som används för att organisera, optimera och strukturera politiska kampanjer ur administrativ och logistisk synvinkel.

(63) Det faktum att ett ***AI-system*** klassificerats som ***ett*** AI-system med hög risk enligt denna förordning bör inte tolkas som att användningen av det systemet är laglig ▌ enligt andra unionsrättsliga akter eller enligt nationell rätt som är förenlig med unionsrätten, exempelvis vad gäller skydd av personuppgifter, användning av lögndetektorer och liknande verktyg eller andra system för att läsa av fysiska personers emotionella tillstånd. All sådan användning bör även fortsättningsvis endast ske i enlighet med de tillämpliga krav som följer av stadgan eller av tillämpliga rättsakter i unionens sekundärrätt och nationell rätt. Denna förordning ska inte tolkas som att den omfattar en rättslig grund för behandling av personuppgifter, inbegripet särskilda kategorier av personuppgifter, i förekommande fall, ***såvida inte annat uttryckligen föreskrivs i denna förordning.***

---

[35] Europaparlamentets och rådets direktiv (EU) 2024/... av den... om transparens och inriktning när det gäller politisk reklam (EUT L,..., ELI: …).

[+] EUT: för in i texten numret på förordningen i PE 90/23 (2021/0381(COD)) och komplettera motsvarande fotnot.

(64) För att begränsa riskerna med AI-system med hög risk som släpps ut ***på marknaden eller*** tas i bruk ***och för att säkerställa hög tillförlitlighet*** bör vissa obligatoriska krav gälla ***för AI-system med hög risk***, med beaktande av ***AI***-systemets avsedda ändamål ***och det sammanhang i vilket det*** används samt i enlighet med det riskhanteringssystem som ska upprättas av leverantören. ***De åtgärder som antas av leverantörerna för att uppfylla de obligatoriska kraven i denna förordning bör ta hänsyn till teknikens allmänt erkända ståndpunkt när det gäller artificiell intelligens och vara proportionerliga och effektiva för att uppnå målen i denna förordning. På grundval av den nya lagstiftningsramen, som klargörs i kommissionens meddelande 2022 års blåbok om genomförandet av EU:s produktbestämmelser, är den allmänna regeln att unionens harmoniseringslagstiftning kan vara tillämplig på en produkt, eftersom tillhandahållandet eller ibruktagandet endast kan ske först när produkten överensstämmer med alla tillämpliga delar av unionens harmoniseringslagstiftning. Riskerna med AI-system som omfattas av kraven i denna förordning rör andra aspekter än unionens befintliga harmoniseringsakter, och därför skulle kraven i denna förordning komplettera det befintliga innehållet i unionens harmoniseringsakter. Maskiner eller medicintekniska produkter som innehåller ett AI-system kan till exempel utgöra risker som inte hanteras genom de grundläggande hälso- och säkerhetskrav som fastställs i unionens berörda harmoniseringslagstiftning, eftersom denna sektorsspecifika lagstiftning inte behandlar risker som är specifika för AI-system.***

Det krävs därför att de olika lagstiftningsakterna tillämpas samtidigt och komplementärt. För att säkerställa konsekvens och undvika en onödig administrativ börda eller onödiga kostnader bör leverantörer av en produkt som innehåller ett eller flera AI-system med hög risk som omfattas av kraven i denna förordning eller i unionens harmoniseringslagstiftning som bygger på den nya lagstiftningsramen i förteckningen i en bilaga till denna förordning vara flexibla när det gäller operativa beslut om hur man på bästa sätt ska säkerställa att en produkt som innehåller ett eller flera AI-system uppfyller alla tillämpliga krav i unionens harmoniseringslagstiftning på ett optimalt sätt. Denna flexibilitet kan till exempel innebära att leverantören beslutar att integrera en del av de nödvändiga testnings- och rapporteringsprocesser, den information och den dokumentation som krävs enligt denna förordning i dokumentation och förfaranden som redan finns och som krävs enligt unionens befintliga harmoniseringslagstiftning som bygger på den nya lagstiftningsramen som förtecknas i en bilaga till denna förordning. Detta bör dock inte på något sätt undergräva leverantörens skyldighet att uppfylla alla tillämpliga krav.

(65) Riskhanteringssystemet bör bestå av en kontinuerlig iterativ process som planeras och löper under hela livscykeln för ett AI-system med hög risk. Denna process bör syfta till att identifiera och begränsa de relevanta riskerna med AI-system för hälsa, säkerhet och grundläggande rättigheter. Riskhanteringssystemet bör regelbundet ses över och uppdateras för att säkerställa dess fortsatta effektivitet samt motivet för och dokumentationen av alla viktiga beslut och åtgärder som vidtas i enlighet med denna förordning. Denna process bör säkerställa att leverantören identifierar risker eller negativa effekter och genomför begränsningsåtgärder för de kända och rimligen förutsebara riskerna med AI-system för hälsa, säkerhet och grundläggande rättigheter mot bakgrund av dess avsedda ändamål och rimligen förutsebar felaktig användning, inbegripet de möjliga risker som uppstår till följd av interaktionen mellan AI-systemet och den miljö där det är i drift. Riskhanteringssystemet bör välja de lämpligaste riskhanteringsåtgärderna mot bakgrund av teknikens ståndpunkt inom AI. Vid identifieringen av de lämpligaste riskhanteringsåtgärderna bör leverantören dokumentera och förklara de val som gjorts och, om relevant, involvera experter och externa berörda parter. Vid identifieringen av den rimligen förutsebara felaktiga användningen av AI-system med hög risk bör leverantören inkludera användningar av AI-system som, även om de inte direkt täcks av det avsedda ändamålet och anges i bruksanvisningen, ändå rimligen kan förväntas bli resultatet av ett lätt förutsägbart mänskligt beteende i samband med det specifika AI-systemets särskilda egenskaper och användning.

Varje känd eller förutsebar omständighet som har samband med användningen av AI-systemet med hög risk i enlighet med dess avsedda ändamål eller under förhållanden med rimligen förutsebar felaktig användning som kan leda till risker för hälsa och säkerhet eller grundläggande rättigheter bör ingå i den bruksanvisning som leverantören tillhandahåller. Syftet med detta är att säkerställa att spridaren är medveten om och tar hänsyn till dessa när AI-systemet med hög risk används. Identifiering och genomförande av riskbegränsningsåtgärder för förutsebar felaktig användning enligt denna förordning bör inte kräva särskilda ytterligare träningsåtgärder för AI-systemet med hög risk från leverantörens sida för att hantera dem. Leverantörerna uppmanas dock att överväga sådana ytterligare träningsåtgärder för att begränsa rimligen förutsebar felaktig användning om de är nödvändiga och lämpliga.

(66) Kraven bör tillämpas på AI-system med hög risk när det gäller ***riskhantering***, kvaliteten på ***och relevansen*** av använda dataset, teknisk dokumentation och arkivering, transparens och information till ***spridarna***, mänsklig tillsyn samt robusthet, noggrannhet och cybersäkerhet. Dessa krav är nödvändiga för att på ett effektivt sätt begränsa riskerna för hälsa, säkerhet och grundläggande rättigheter, ▌ och inga andra åtgärder som är mindre handelsbegränsande finns rimligen tillgängliga, så att omotiverade begränsningar av handeln motverkas.

(67) ***Data av hög kvalitet och tillgången till data av hög*** kvalitet ***spelar en avgörande roll när det gäller att tillhandahålla struktur och att säkerställa*** många AI-systems prestanda, i synnerhet vid användning av teknik som förutsätter träning av modeller för att säkerställa att AI-system med hög risk fungerar säkert och på avsett sätt och inte blir ***en*** källa till diskriminering som är förbjuden enligt unionsrätten. Högkvalitativa ***dataset för träning, validering och testning förutsätter genomförande av lämpliga metoder för dataförvaltning och datahantering***. ***Dataset för träning, validering och testning, inbegripet märkningarna, bör vara relevanta, tillräckligt representativa och i största möjliga utsträckning*** fria från fel och fullständiga med tanke på systemets avsedda ändamål. ***För att underlätta efterlevnaden av unionens dataskyddslagstiftning, såsom förordning (EU) 2016/679, bör dataförvaltnings- och datahanteringsmetoderna när det gäller personuppgifter inbegripa transparens om det ursprungliga syftet med uppgiftsinsamlingen. Dataseten*** bör också ha lämpliga statistiska egenskaper, även när det gäller de personer eller grupper av personer ***i fråga om vilka*** AI-systemet med hög risk är avsett att användas***, med särskild uppmärksamhet på att begränsa eventuella snedvridningar i dataseten som sannolikt påverkar människors hälsa och säkerhet, inverkar negativt på grundläggande rättigheter eller leder till diskriminering som är förbjuden enligt unionsrätten, särskilt när utdata påverkar indata för framtida operationer (”återföring”). Snedvridningar kan exempelvis vara inneboende i underliggande dataset, särskilt när historiska data används eller genereras när systemen tillämpas i verkliga sammanhang.***

De resultat som AI-system ger kan påverkas av sådana inneboende snedvridningar som tenderar att gradvis öka och därigenom vidmakthålla och förstärka den befintliga diskrimineringen, särskilt för sårbara personer som tillhör vissa grupper, inbegripet rasgrupper eller etniska grupper. Kravet på att dataseten i största möjliga utsträckning ska vara fullständiga och fria från fel bör inte påverka användningen av integritetsbevarande teknik i samband med utveckling och testning av AI-system. I synnerhet bör dataset, i den mån som krävs för deras avsedda ändamål, ***beakta*** funktioner, särdrag eller element som är specifika för den särskilda geografiska, ***kontextuella***, beteendemässiga eller funktionsmässiga situation där AI-systemet är avsett att användas. ***De krav som rör dataförvaltning kan uppfyllas genom att tredje parter anlitas som erbjuder certifierade tjänster för uppfyllelse av kraven, inbegripet kontroll av dataförvaltning, datasetens integritet och metoder för träning, validering och testning av data, i den mån överensstämmelse med uppgiftskraven i denna förordning säkerställs.***

(68) För utvecklingen ***och bedömningen*** av AI-system med hög risk bör vissa aktörer, såsom leverantörer, anmälda organ och andra berörda enheter – exempelvis digitala innovationsknutpunkter, test- och experimentanläggningar och forskare – kunna få åtkomst till och använda dataset av hög kvalitet inom sina respektive verksamhetsområden som är relaterade till denna förordning. Gemensamma europeiska dataområden som inrättas av kommissionen och främjande av datadelning mellan företag och med offentlig förvaltning i allmänhetens intresse kommer att vara avgörande för tillhandahållandet av förtroendefull, ansvarsskyldig och icke-diskriminerande åtkomst till högkvalitativa data för träning, validering och testning av AI-system. På exempelvis hälsoområdet kommer det europeiska hälsodataområdet att främja icke-diskriminerande åtkomst till hälsodata och träning av AI-algoritmer på dessa dataset, på ett sätt som bevarar den personliga integriteten och är säkert, snabbt, transparent och tillförlitligt och med lämpliga institutionella styrelseformer. Berörda behöriga myndigheter, även sektorsbaserade sådana, som tillhandahåller eller stöder åtkomst till data får också stödja tillhandahållandet av högkvalitativa data för träning, validering och testning av AI-system.

(69) Rätten till integritet och skydd av personuppgifter måste garanteras under AI-systemets hela livscykel. I detta avseende är principerna om uppgiftsminimering och inbyggt dataskydd och dataskydd som standard, i enlighet med unionens dataskyddslagstiftning, tillämpliga när personuppgifter behandlas. De åtgärder som leverantörerna vidtar för att säkerställa efterlevnaden av dessa principer får omfatta inte bara anonymisering och kryptering, utan även användning av teknik som gör det möjligt att föra in algoritmer i data och möjliggöra träning av AI-system utan överföring mellan parter eller kopiering av rådata eller strukturerade data i sig, utan att det påverkar tillämpningen av de krav på dataförvaltning som föreskrivs i denna förordning.

(70) För att skydda andras rätt att slippa diskriminering som kan följa av snedvridning i AI-system, bör leverantörerna undantagsvis, i den utsträckning det är absolut nödvändigt för att säkerställa upptäckt och korrigering av snedvridning i samband med AI-systemen med hög risk, med förbehåll för lämpliga skyddsåtgärder för fysiska personers grundläggande rättigheter och friheter och enligt tillämpningen av alla tillämpliga villkor som fastställs i denna förordning och i förordningarna (EU) 2016/679, (EU) 2018/1725 och (EU) nr 2016/680 kunna behandla även särskilda kategorier av personuppgifter, som en fråga av betydande allmänintresse, i den mening som avses i artikel 9.2 g i förordning (EU) 2016/679 och artikel 10.2 g i förordning (EU) 2018/1725.

(71) Det är mycket viktigt att ha ***begriplig*** information om hur AI-system med hög risk har utvecklats och hur de presterar under hela sin ***livstid***, för att ***möjliggöra att dessa system är spårbara***, kontrollera att kraven enligt denna förordning uppfylls ***samt kunna utföra övervakning av deras drift och övervakning efter utsläppande på marknaden***. Detta förutsätter arkivering och tillgång till teknisk dokumentation som innehåller den information som krävs för att bedöma om AI-systemet uppfyller de berörda kraven ***och underlätta övervakning efter utsläppande på marknaden***. Denna information bör innefatta systemets allmänna egenskaper, kapacitet och begränsningar samt algoritmer, data, de förfaranden som används för träning, testning och validering samt dokumentation av relevanta riskhanteringssystem ***och ha utformats i klar och begriplig form***. Den tekniska dokumentationen bör vara lämpligt uppdaterad ***under hela AI-systemets livstid***. ***AI-system med hög risk bör dessutom tekniskt möjliggöra automatisk registrering av händelser genom loggar under systemets livstid.***

(72) För att ta itu med ***farhågor som hör samman med*** den bristande insynen ***och komplexiteten*** i vissa AI-system ***och göra det lättare för spridarna att fullgöra sina skyldigheter enligt denna förordning*** bör transparens krävas för AI-system med hög risk ***innan de släpps ut på marknaden eller tas i bruk***. ***AI-system med hög risk*** bör ***utformas på ett sätt som gör det möjligt för spridare att förstå hur AI***-systemet ***fungerar, utvärdera dess funktionalitet och förstå dess styrkor och begränsningar***. AI-system ***med hög risk*** bör ▌ åtföljas av ***lämplig information i form av*** bruksanvisningar. ***Sådan information bör omfatta AI-systemets egenskaper, kapacitet och prestandabegränsningar. Sådana element skulle omfatta*** information ***om eventuella kända och förutsebara omständigheter som har samband med användningen av AI-systemet med hög risk,*** inbegripet ***spridares åtgärder som kan påverka systemets beteende och prestanda, under vilka AI-systemet kan leda till*** risker för ***hälsa, säkerhet och*** grundläggande rättigheter***, om de förändringar som på förhand har fastställts och bedömts för överensstämmelse av leverantören och om relevanta åtgärder för mänsklig tillsyn, inbegripet åtgärderna för att underlätta spridarnas tolkning av AI-systemets utdata. Öppenhet, inklusive åtföljande bruksanvisningar bör hjälpa spridarna att använda systemet och stödja deras välgrundade beslutsfattande. Spridare bör bland annat ha bättre förutsättningar att göra rätt val av vilket system de avser att använda mot bakgrund av de skyldigheter som gäller för dem, få kunskap om avsedd och utesluten användning samt använda AI-systemet korrekt och när så är lämpligt. För att förbättra läsbarheten och tillgängligheten för den information som ingår i bruksanvisningen bör,*** när så är lämpligt***, belysande exempel om exempelvis begränsningar och om avsedd och utesluten användning av AI-systemet, inkluderas. Leverantörerna bör säkerställa att all dokumentation, inbegripet bruksanvisningen, innehåller meningsfull, heltäckande, tillgänglig och begriplig information, med beaktande av de behov och den förmodade kunskap som de spridare som man riktar sig till har. Bruksanvisningen bör tillhandahållas på ett språk som lätt kan förstås av de spridare som man riktar sig till, i enlighet med vad som fastställs av den berörda medlemsstaten.***

(73) AI-system med hög risk bör utformas och utvecklas på ett sådant sätt att fysiska personer kan övervaka deras funktionssätt***, säkerställa att de används som avsett och att deras effekter hanteras under systemets livscykel***. Därför bör lämpliga åtgärder för mänsklig tillsyn identifieras av leverantören av systemet innan detta släpps ut på marknaden eller tas i bruk. Sådana åtgärder bör i synnerhet, när så är lämpligt, garantera att systemet är föremål för inbyggda operativa begränsningar som inte systemet själv kan åsidosätta och lyder den mänskliga operatören, och att de fysiska personer som anförtros uppgiften att utöva mänsklig tillsyn har den kompetens, utbildning och auktoritet som de behöver för att utföra sina uppgifter. ***Det är också viktigt, beroende på vad som är lämpligt, att säkerställa att AI-system med hög risk innehåller mekanismer för att vägleda och informera den fysiska person som anförtros uppgiften att utöva mänsklig tillsyn när det gäller att fatta välgrundade beslut om, när och hur man ska ingripa för att undvika negativa konsekvenser eller risker eller stoppa systemet om det inte fungerar som avsett. Med tanke på de betydande konsekvenserna för personer vid vissa biometriska identifieringssystems felaktiga träffar är det lämpligt att föreskriva ett förstärkt krav på mänsklig tillsyn för dessa system så att spridaren inte kan vidta åtgärder eller fatta beslut på grundval av den identifiering som systemet ger upphov till, såvida inte detta har verifierats och bekräftats separat av minst två fysiska personer. Dessa personer kan komma från en eller flera enheter och inbegripa den person som driver eller använder systemet. Detta krav bör inte medföra onödiga bördor eller förseningar och det kan vara tillräckligt att de olika personernas separata kontroller automatiskt registreras i de loggar som genereras av systemet. Med tanke på särdragen inom brottsbekämpning, migration, gränskontroll och asyl bör detta krav inte tillämpas i fall där tillämpningen av detta krav enligt unionsrätten eller nationell rätt betraktas som oproportionerlig.***

(74) AI-system med hög risk bör fungera konsekvent under hela sin livscykel och uppnå en lämplig nivå av noggrannhet, robusthet och cybersäkerhet ***i ljuset av sitt avsedda ändamål och*** i enlighet med teknikens allmänt erkända ståndpunkt. ***Kommissionen och relevanta organisationer och berörda parter uppmanas att ta vederbörlig hänsyn till riskbegränsning och AI-systemets negativa konsekvenser. Den förväntade*** graden av ***prestandamått bör anges i den medföljande bruksanvisningen***. ***Leverantörerna uppmanas att förmedla denna information till spridarna på ett tydligt och lättbegripligt sätt, utan missförstånd eller vilseledande uttalanden. Unionslagstiftningen om legal metrologi, inbegripet Europaparlamentets och rådets direktiv 2014/31/EU [36]och 2014/32/EU[37], syftar till att säkerställa mätningarnas noggrannhet och att bidra till öppenhet och rättvisa i handelstransaktioner. I detta sammanhang bör kommissionen, i samarbete med relevanta berörda parter och organisationer, såsom metrologi- och riktmärkningsmyndigheter, vid behov uppmuntra utvecklingen av riktmärken och mätmetoder för AI-system. Därvid bör kommissionen följa och samarbeta med internationella partner som arbetar med metrologi och relevanta mätindikatorer som rör artificiell intelligens.***

---

36 Europaparlamentets och rådets direktiv 2014/31/EU av den 26 februari 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av icke-automatiska vågar (EUT L 96, 29.3.2014, s. 107).

37 Europaparlamentets och rådets direktiv 2014/32/EU av den 26 februari 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av mätinstrument (EUT L 96, 29.3.2014, s. 149).

(75) Teknisk robusthet är ett nyckelkrav för AI-system med hög risk. De bör vara resilienta ***mot skadligt eller på annat sätt oönskat beteende som kan bero på*** begränsningar ***inom de system eller den miljö där systemen fungerar*** (t.ex. felaktigheter, funktionsfel, inkonsekvenser, oväntade situationer). ***Därför bör tekniska och organisatoriska åtgärder vidtas för att säkerställa robustheten i AI-system med hög risk, till exempel genom att utforma och utveckla lämpliga tekniska lösningar för att förebygga eller minimera*** skadligt eller på annat sätt oönskat beteende. ***Dessa tekniska lösningar kan till exempel omfatta mekanismer som gör det möjligt för systemet att på ett säkert sätt avbryta sin drift (felsäkra planer) vid vissa avvikelser eller när driften sker utanför vissa på förhand fastställda gränser.*** Bristande skydd mot dessa risker kan leda till säkerhetskonsekvenser eller inverka negativt på grundläggande rättigheter, exempelvis på grund av felaktiga beslut eller felaktiga eller snedvridna utdata som genereras av AI-systemet.

(76) Cybersäkerhet har avgörande betydelse för att säkerställa att AI-systemen är resilienta mot försök att ändra deras användning, beteende eller prestanda eller att undergräva deras säkerhetsegenskaper genom tredje parter med avsikt att vålla skada som utnyttjar systemets svagheter. Cyberattacker mot AI-system kan riktas mot AI-specifika tillgångar, såsom träningsdataset (t.ex. dataförgiftning) eller tränade modeller (t.ex. antagonistiska attacker ***eller medlemskapsinferens***), eller utnyttja sårbarheter i AI-systemets digitala tillgångar eller i den underliggande IKT-infrastrukturen. För att säkerställa en cybersäkerhetsnivå som är anpassad till riskerna bör sådana lämpliga åtgärder ***som säkerhetskontroller*** därför vidtas av leverantörerna av AI-system med hög risk, även med beaktande av den underliggande IKT-infrastrukturen, när så är lämpligt.

(77) Utan att det påverkar de krav avseende robusthet och noggrannhet som fastställs i denna förordning kan AI-system med hög risk som omfattas av tillämpningsområdet för Europaparlamentets och rådets förordning (EU) 2024/...[38+] i enlighet med artikel 8 i den förordningen visa överensstämmelse med cybersäkerhetskraven i denna förordning genom att uppfylla de grundläggande cybersäkerhetskrav som anges i artikel 10 i och bilaga I till förordning (EU) 2024/…[++]. Om AI-system med hög risk uppfyller de grundläggande kraven i förordning (EU) 2024/…[++], bör de anses uppfylla de cybersäkerhetskrav som fastställs i den här förordningen, i den mån uppfyllandet av dessa krav visas i den EU-försäkran om överensstämmelse eller delar av den som utfärdats i enlighet med förordning (EU) 2024/…[++]. I detta syfte bör den bedömning av cybersäkerhetsrisker som är förknippade med en produkt med digitala element som klassificeras som AI-system med hög risk i enlighet med denna förordning och som utförs i enlighet med förordning (EU) 2024/…[++], beakta risker för ett AI-systems cyberresiliens när det gäller obehöriga tredje parters försök att ändra dess användning, beteende eller prestanda, inbegripet AI-specifika sårbarheter såsom dataförgiftning eller antagonistiska attacker, samt, i relevanta fall, risker för grundläggande rättigheter i enlighet med kraven i den här förordningen.

---

38 Europaparlamentets och rådets förordning (EU) 2024/... av den... om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020 (EUT L,..., ELI: …).

+ EUT: För in i texten numret på förordningen i PE XX/YY (2022/0272 (COD)) och komplettera motsvarande fotnot.

(78) Det förfarande för bedömning av överensstämmelse som föreskrivs i denna förordning bör tillämpas på de grundläggande cybersäkerhetskraven för en produkt med digitala element som omfattas av förordning (EU) 2024/...[+] och som klassificeras som ett AI-system med hög risk enligt denna förordning. Denna regel bör dock inte leda till att den nödvändiga assuransnivån sänks för kritiska produkter med digitala element som omfattas av förordning (EU) 2024/…[+]. Med avvikelse från denna regel omfattas därför också AI-system med hög risk som omfattas av denna förordning och som också kategoriseras som viktiga eller kritiska produkter med digitala element enligt förordning (EU) 2024/…[+], och på vilka förfarandet för bedömning av överensstämmelse baserat på intern kontroll enligt en bilaga till denna förordning är tillämpligt, av bestämmelserna om bedömning av överensstämmelse i förordning (EU) 2024/…[+] i den mån som de grundläggande cybersäkerhetskraven i den förordningen berörs. Om så är fallet bör de respektive bestämmelserna om bedömning av överensstämmelse på grundval av intern kontroll i en bilaga till denna förordning gälla för alla andra aspekter som omfattas av denna förordning. Med utgångspunkt i Enisas kunskap och expertis om den cybersäkerhetspolicy och de uppgifter som tilldelats Enisa enligt förordning (EU) 2019/1020 bör kommissionen samarbeta med Enisa i frågor som rör cybersäkerhet i AI-system.

[+] EUT: för in numret på förordningen i PE XX/YY (2022/0272 (COD)).

()

(79) Det är lämpligt att en specifik fysisk eller juridisk person, definierad som leverantören, tar ansvaret för utsläppande på marknaden eller ibruktagandet av ett AI-system med hög risk, oavsett om denna fysiska eller juridiska person är den person som utformat eller utvecklat systemet.

(80) ***Som signatärer av FN:s konvention om rättigheter för personer med funktionsnedsättning är unionen och alla medlemsstater rättsligt förpliktigade att skydda personer med funktionsnedsättning från diskriminering och främja deras jämlikhet, att säkerställa att personer med funktionsnedsättning på lika villkor som andra har tillgång till informations- och kommunikationsteknik och informations- och kommunikationssystem samt att säkerställa att integriteten hos personer med funktionsnedsättning respekteras. Med tanke på den ökande betydelsen och användningen av AI-system bör tillämpningen av universella konstruktionsprinciper för all ny teknik och alla nya tjänster säkerställa fullständig och jämlik tillgång för alla som potentiellt påverkas av eller använder AI-teknik, inbegripet personer med funktionsnedsättning, på ett sätt som tar full hänsyn till deras inneboende värdighet och mångfald. Det är därför viktigt att leverantörerna säkerställer full överensstämmelse med tillgänglighetskraven, inbegripet Europaparlamentets och rådets direktiv (EU) 2016/2102[39] och direktiv (EU) 2019/882. Leverantörerna bör säkerställa att dessa krav uppfylls genom utformning. Därför bör de nödvändiga åtgärderna i så stor utsträckning som möjligt integreras i utformningen av AI-systemet med hög risk.***

[39] Europaparlamentets och rådets direktiv (EU) 2016/2102 av den 26 oktober 2016 om tillgänglighet avseende offentliga myndigheters webbplatser och mobila applikationer (EUT L 327, 2.12.2016, s. 1).

(81) Leverantören bör inrätta ett sunt kvalitetsstyrningssystem, säkerställa att det föreskrivna förfarandet för bedömning av överensstämmelse genomförs, utarbeta den relevanta dokumentationen och inrätta ett robust system för övervakning efter utsläppande på marknaden. ***Leverantörer av AI-system med hög risk som omfattas av skyldigheter avseende kvalitetsstyrningssystem enligt relevant sektorsspecifik unionslagstiftning bör ha möjlighet att inkludera delarna av det kvalitetsstyrningssystem som föreskrivs i denna förordning som en del av befintliga kvalitetsstyrningssystem som föreskrivs i nämnda sektorsspecifika unionslagstiftning. Komplementariteten mellan denna förordning och befintlig sektorsspecifik unionslagstiftning bör också beaktas i framtida standardiseringsverksamhet eller vägledning som antas av kommissionen.*** Offentliga myndigheter som för egen användning tar i bruk AI-system med hög risk kan anta och genomföra reglerna för kvalitetsstyrningssystem som en del av det kvalitetsstyrningssystem som införs på nationell eller regional nivå, beroende på vad som är lämpligt, med beaktande av sektorns särdrag och den berörda offentliga myndighetens kompetensområde och organisation.

(82) För att möjliggöra kontrollen av efterlevnaden av denna förordning och skapa lika villkor för operatörerna, och med beaktande av de olika formerna för att tillhandahålla digitala produkter, är det viktigt att säkerställa att en person som är etablerad i unionen under alla omständigheter kan förse myndigheterna med all den information om AI-systemens överensstämmelse som är nödvändig. Innan ▌ leverantörer etablerade i tredjeländer tillhandahåller sina AI-system i unionen bör de genom skriftlig fullmakt utse ett ombud som är etablerat i unionen. ***Detta ombud har en central roll för att säkerställa att de AI-system med hög risk som släpps ut på marknaden eller tas i bruk av de leverantörer som inte är etablerade i unionen uppfyller kraven och för att fungera som leverantörernas kontaktpersoner etablerade i unionen.***

(83) Mot bakgrund av karaktären hos och komplexiteten i värdekedjan för AI-system och i linje med den nya lagstiftningsramens principer är det viktigt att säkerställa rättssäkerheten och underlätta efterlevnaden av denna förordning. Det är därför nödvändigt att klargöra rollen och de särskilda skyldigheterna för berörda operatörer längs värdekedjan, såsom importörer och distributörer som kan bidra till utvecklingen av AI-system. I vissa situationer kan dessa operatörer agera i mer än en roll samtidigt och bör därför kumulativt fullgöra alla relevanta skyldigheter med anknytning till dessa roller. En operatör kan till exempel samtidigt agera som distributör och importör.

(84) ***För att säkerställa rättssäkerhet är det nödvändigt att klargöra att under vissa*** särskilda ***villkor bör varje distributör, importör, spridare eller annan tredje part betraktas som leverantör av ett AI-system med hög risk och därför åta sig alla relevanta*** skyldigheter. ***Detta skulle vara fallet om den parten sätter sitt namn eller varumärke på ett AI-system med hög risk som redan släppts ut på marknaden eller tagits i bruk, utan att det påverkar avtalsarrangemang som föreskriver att skyldigheterna tilldelas på annat sätt, eller om den parten gör en väsentlig ändring av ett AI-system med hög risk som redan släppts ut på marknaden eller redan tagits i bruk och på ett sätt som innebär att det förblir ett AI-system med hög risk i enlighet med denna förordning, eller om den ändrar det avsedda ändamålet med ett AI-system, inbegripet ett AI-system för allmänna ändamål, som inte har klassificerats som system med hög risk och som redan släppts ut på marknaden eller tagits i bruk, på ett sätt som innebär att AI-systemet blir ett AI-system med hög risk i enlighet med denna förordning. Dessa bestämmelser bör tillämpas utan att det påverkar tillämpningen av mer specifika bestämmelser som fastställs i vissa delar av unionens harmoniseringslagstiftning som bygger på den nya lagstiftningsramen, med vilken denna förordning bör tillämpas gemensamt. Till exempel bör artikel 16.2 i förordning (EU) 2017/745, där det fastställs att vissa ändringar inte*** bör ***anses vara en ändring av en produkt som kan påverka dess överensstämmelse med de tillämpliga kraven, fortsätta att tillämpas på AI-system med hög risk som är medicintekniska produkter i den mening som avses i den förordningen***.

(85) AI-system för allmänna ändamål kan själva användas som AI-system med hög risk eller kan vara komponenter i andra AI-system med hög risk. Därför bör leverantörerna av sådana system, på grund av systemens särskilda karaktär och för att säkerställa en rättvis ansvarsfördelning längs AI-värdekedjan, oavsett om systemen som sådana kan användas som AI-system med hög risk av andra leverantörer eller som komponenter i AI-system med hög risk och utom i de fall annat föreskrivs i denna förordning, ha ett nära samarbete med leverantörerna av de berörda AI-systemen med hög risk för att göra det möjligt för dem att uppfylla de relevanta skyldigheterna enligt denna förordning och rätta sig efter de behöriga myndigheter som inrättats enligt denna förordning.

(86) Om den leverantör som ursprungligen släppte ut AI-systemet på marknaden eller tog det i bruk, i enlighet med de villkor som fastställs i denna förordning, inte längre bör anses vara leverantör vid tillämpning av denna förordning, och om denna leverantör inte uttryckligen har uteslutit omvandlingen av AI-systemet till ett AI-system med hög risk, bör den förstnämnda leverantören detta till trots ha ett nära samarbete och tillgängliggöra den nödvändiga informationen och tillhandahålla den rimligen förväntade tekniska åtkomsten och annat stöd som krävs för att fullgöra de skyldigheter som fastställs i denna förordning, särskilt när det gäller efterlevnaden av bedömningen av överensstämmelse för AI-system med hög risk.

(87) Om ett AI-system med hög risk som ingår som säkerhetskomponent i en produkt som omfattas av unionens harmoniseringslagstiftning som bygger på den nya lagstiftningsramen inte släpps ut på marknaden och inte heller tas i bruk fristående från produkten, bör den produkttillverkaren som definieras i den lagstiftningen fullgöra de leverantörsskyldigheter som fastställs i denna förordning och i synnerhet säkerställa att det AI-system som ingår i slutprodukten uppfyller kraven i denna förordning.

(88) Inom AI-värdekedjan tillhandahåller flera parter ofta AI-system, verktyg och tjänster, men även komponenter eller processer som leverantören integrerar i AI-systemet för olika ändamål som bland annat omfattar träning, omträning, testning och utvärdering av modeller samt integrering i programvara eller andra aspekter av modellutveckling. Dessa parter intar en viktig roll i värdekedjan gentemot leverantören av AI-systemet med hög risk i vilken deras AI-system, verktyg, tjänster, komponenter eller processer är integrerade, och bör genom skriftligt avtal tillhandahålla denna leverantör nödvändig information, kapacitet, teknisk åtkomst och annat stöd baserat på teknikens allmänt erkända ståndpunkt, för att göra det möjligt för leverantören att fullt ut uppfylla de skyldigheter som fastställs i denna förordning, utan att äventyra sina egna immateriella rättigheter eller företagshemligheter.

(89) Tredjeparter som för allmänheten tillgängliggör andra verktyg, tjänster, processer eller AI-komponenter än AI-modeller för allmänna ändamål ska inte åläggas att uppfylla krav som är inriktade på ansvarsområdena längs AI-värdekedjan, särskilt gentemot den leverantör som har använt eller integrerat dem, när dessa verktyg, tjänster, processer eller AI-komponenter görs tillgängliga med en fri och öppen licens. Utvecklare av fria verktyg, tjänster eller processer med öppen källkod, eller andra AI-modeller än AI-modeller för allmänna ändamål, bör uppmuntras att tillämpa allmänt vedertagen dokumentationspraxis, såsom modellkort och datablad, som ett sätt att påskynda informationsutbytet längs AI-värdekedjan, vilket gör det möjligt att främja tillförlitliga AI-system i unionen.

(90) Kommissionen kan utveckla och rekommendera frivilliga standardavtalsvillkor mellan leverantörer av AI-system med hög risk och tredje parter som tillhandahåller verktyg, tjänster, komponenter eller processer som används eller är integrerade i AI-system med hög risk för att underlätta samarbetet längs värdekedjan. Vid utarbetandet av frivilliga standardavtalsvillkor bör kommissionen också ta hänsyn till eventuella avtalskrav som är tillämpliga inom specifika sektorer eller affärsfall.

(91) Mot bakgrund av AI-systemens natur och de risker för säkerhet och grundläggande rättigheter som kan vara förknippade med användningen av dem, inbegripet när det gäller behovet av att säkerställa en korrekt övervakning av ett AI-systems prestanda under verkliga förhållanden, är det lämpligt att fastställa särskilda ansvarsområden för ***spridarna***. ***Spridarna*** bör i synnerhet ***vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att de*** använder AI-system med hög risk i enlighet med bruksanvisningarna, och vissa andra skyldigheter bör föreskrivas när det gäller övervakning av AI-systemens funktionssätt och i fråga om arkivering, på lämpligt sätt. ***Spridarna bör dessutom säkerställa att de personer som anförtros uppgiften att genomföra bruksanvisningarna och den mänskliga tillsynen enligt denna förordning har den kompetens som krävs, särskilt en lämplig nivå av AI-kunskap, utbildning och befogenhet för att korrekt fullgöra dessa uppgifter. Dessa skyldigheter bör inte påverka andra spridarskyldigheter i samband med AI-system med hög risk enligt unionsrätten eller nationell rätt.***

(92) ***Denna förordning påverkar inte arbetsgivarnas skyldigheter att informera eller att informera och samråda med arbetstagare eller deras företrädare enligt unionsrätten eller nationell rätt och praxis, inbegripet Europaparlamentets och rådets direktiv 2002/14/EG[40] om inrättande av en allmän ram för information till och samråd med arbetstagare, om beslut att ta i bruk eller använda AI-system. Det måste fortfarande säkerställas att arbetstagarna och deras företrädare informeras om det planerade införandet av AI-system med hög risk på arbetsplatsen i de fall där villkoren för dessa informations- eller informations- och samrådsskyldigheter i andra rättsliga instrument inte är uppfyllda. Denna rätt till information är dessutom underordnad och nödvändig för att skydda de grundläggande rättigheter som ligger till grund för denna förordning. Därför bör ett informationskrav för detta fastställas i denna förordning utan att det påverkar arbetstagarnas befintliga rättigheter.***

[40] Europaparlamentets och rådets direktiv 2002/14/EG av den 11 mars 2002 om inrättande av en allmän ram för information till och samråd med arbetstagare i Europeiska gemenskapen – Gemensamt uttalande av Europaparlamentet, rådet och kommissionen om arbetstagarrepresentation (EGT L 80, 23.3.2002, s. 29).

(93) Riskerna med avseende på AI-system kan ha att göra med hur systemen utformas, men de kan även härröra från hur dessa AI-system används. Spridare av AI-system med hög risk spelar därför en avgörande roll när det gäller att säkerställa att de grundläggande rättigheterna skyddas, och kompletterar leverantörens skyldigheter vid utvecklingen av AI-systemet. Spridare är bäst på att förstå hur AI-system med hög risk kommer att användas konkret och kan därför fastställa potentiella risker som inte har förutsetts under utvecklingsfasen, tack vare mer exakt kunskap om sammanhanget för användningen och de personer eller grupper av personer som sannolikt kommer att påverkas, däribland grupper av sårbara personer. Spridare av AI-system med hög risk som avses i en bilaga till denna förordning spelar också en avgörande roll när det gäller att informera fysiska personer och bör när de fattar beslut eller hjälper till att fatta beslut som rör fysiska personer i förekommande fall informera de fysiska personerna om att de är föremål för användning av AI-systemet med hög risk. Denna information bör omfatta det avsedda ändamålet och typen av beslut som det fattar. Spridaren bör också informera den fysiska personen om dennes rätt till en förklaring enligt denna förordning. När det gäller AI-system med hög risk som används för brottsbekämpningsändamål bör denna skyldighet genomföras i enlighet med artikel 13 i direktiv (EU) 2016/680.

(94) All behandling av biometriska uppgifter som ingår i användningen av AI-system för biometrisk identifiering för brottsbekämpning måste vara förenlig med artikel 10 i direktiv (EU) 2016/680, som medger sådan behandling endast när det är absolut nödvändigt, med förbehåll för lämpliga skyddsåtgärder för den registrerades rättigheter och friheter, och när detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt. När sådan användning är tillåten måste den också respektera de principer som fastställs i artikel 4.1 i direktiv (EU) 2016/680, inbegripet laglighet, rättvisa och öppenhet, ändamålsbegränsning, korrekthet och lagringsbegränsning.

(95) Utan att det påverkar tillämplig unionsrätt, särskilt förordning (EU) 2016/679 och direktiv (EU) 2016/680, bör användningen av system för biometrisk fjärridentifiering i efterhand omfattas av skyddsåtgärder, med tanke på den inkräktande karaktären hos system för biometrisk fjärridentifiering i efterhand. System för biometrisk identifiering i efterhand bör alltid användas på ett sätt som är proportionerligt, legitimt och strikt nödvändigt och därmed målinriktat, när det gäller de personer som ska identifieras, plats och tidsmässig omfattning samt baserat på ett slutet dataset av lagligen förvärvade videoupptagningar. Under alla omständigheter bör system för biometrisk fjärridentifiering i efterhand inte användas inom ramen för brottsbekämpning för att leda till urskillningslös övervakning. Villkoren för biometrisk fjärridentifiering i efterhand bör under inga omständigheter utgöra en grund för att kringgå villkoren för förbudet och de strikta undantagen för biometrisk fjärridentifiering i realtid.

(96) För att effektivt säkerställa att de grundläggande rättigheterna skyddas bör spridare av AI-system med hög risk som är offentligrättsliga organ, eller privata aktörer som tillhandahåller offentliga tjänster och operatörer som sprider vissa AI-system med hög risk som förtecknas i en bilaga till denna förordning, såsom bank- eller försäkringsenheter, genomföra en konsekvensbedömning avseende grundläggande rättigheter innan systemen tas i bruk. Tjänster som är viktiga för enskilda personer och som är av offentlig karaktär kan också tillhandahållas av privata enheter. Privata aktörer som tillhandahåller sådana tjänster av offentlig karaktär är kopplade till uppgifter av allmänt intresse, såsom utbildning, hälso- och sjukvård, sociala tjänster, bostäder och rättsskipning. Syftet med konsekvensbedömningen avseende grundläggande rättigheter är att spridaren ska identifiera de specifika riskerna för rättigheterna för enskilda personer eller grupper av enskilda personer som sannolikt kommer att beröras och identifiera åtgärder som ska vidtas om dessa risker förverkligas. Konsekvensbedömningen bör tillämpas på den första användningen av AI-systemet med hög risk och bör uppdateras när spridaren anser att någon av de relevanta faktorerna har förändrats. Konsekvensbedömningen bör identifiera spridarens relevanta processer där AI-systemet med hög risk kommer att användas i linje med dess avsedda ändamål, och bör innehålla en beskrivning av den tidsperiod under vilken och den frekvens med vilken systemet är avsett att användas samt av specifika kategorier av fysiska personer och grupper som sannolikt kommer att påverkas i det specifika användningssammanhanget.

Bedömningen bör också omfatta identifiering av särskilda risker för skada som sannolikt kommer att påverka dessa personers eller gruppers grundläggande rättigheter. Vid utförandet av denna bedömning bör spridaren beakta information som är relevant för en korrekt konsekvensbedömning, inbegripet men inte begränsat till den information som tillhandahålls av leverantören av AI-systemet med hög risk i bruksanvisningen. Mot bakgrund av de risker som identifierats bör spridarna fastställa vilka åtgärder som ska vidtas om dessa risker förverkligas, inbegripet till exempel styrningsformer i det specifika användningssammanhanget, såsom arrangemang för mänsklig tillsyn i enlighet med bruksanvisningen eller klagomålshanteringsförfaranden och prövningsförfaranden, eftersom de kan vara avgörande för att bidra till att begränsa riskerna för de grundläggande rättigheterna i konkreta användningsfall. Efter att ha utfört denna konsekvensbedömning bör spridaren underrätta den berörda marknadskontrollmyndigheten. För att samla in relevant information som är nödvändig för att utföra konsekvensbedömningen kan spridare av AI-system med hög risk, särskilt när AI-system används i den offentliga sektorn, involvera relevanta berörda parter, inbegripet företrädare för grupper av personer som sannolikt kommer att påverkas av AI-systemet, oberoende experter och organisationer i det civila samhället i genomförandet av sådana konsekvensbedömningar och utformningen av åtgärder som ska vidtas om riskerna förverkligas. Europeiska byrån för artificiell intelligens (AI-byrån) bör utarbeta en mall för ett frågeformulär för att underlätta efterlevnad och minska den administrativa bördan för spridare.

(97) För att skapa rättssäkerhet bör begreppet AI-modeller för allmänna ändamål definieras tydligt och särskiljas från begreppet AI-system. Definitionen bör baseras på de viktigaste funktionella egenskaperna hos en AI-modell för allmänna ändamål, generaliteten och förmågan att på ett kompetent sätt utföra ett stort antal olika uppgifter. Dessa modeller tränas vanligtvis med stora mängder data genom olika metoder, såsom självövervakad inlärning, oövervakad inlärning eller återkopplingsinlärning. AI-modeller för allmänna ändamål får släppas ut på marknaden på olika sätt, bland annat genom bibliotek, gränssnitt för applikationsprogrammering, som direkt nedladdning eller som fysisk kopia. Dessa modeller kan ändras ytterligare eller finjusteras till nya modeller. Även om AI-modeller är väsentliga komponenter i AI-system utgör de inte AI-system i sig. AI-modeller kräver tillägg av ytterligare komponenter, till exempel ett användargränssnitt, för att bli AI-system. AI-modeller är vanligtvis integrerade i och utgör en del av AI-system. I denna förordning fastställs särskilda regler för AI-modeller för allmänna ändamål och för AI-modeller för allmänna ändamål som medför systemrisker, vilka bör gälla även när dessa modeller är integrerade eller ingår i ett AI-system. Det bör förstås att skyldigheterna för leverantörer av AI-modeller för allmänna ändamål bör gälla när AI-modellerna för allmänna ändamål släpps ut på marknaden.

När leverantören av en AI-modell för allmänna ändamål integrerar en egen modell i sitt eget AI-system som tillhandahålls på marknaden eller tas i bruk, bör den modellen anses ha släppts ut på marknaden, och skyldigheterna i denna förordning för modeller bör därför fortsätta att gälla utöver skyldigheterna för AI-system. De skyldigheter som föreskrivs för modeller bör under alla omständigheter inte gälla när en egen modell används för rent interna processer som inte är väsentliga för att tillhandahålla en produkt eller tjänst till tredje parter och fysiska personers rättigheter inte påverkas. Med tanke på att de har potentiellt betydande negativa effekter bör AI-modeller för allmänna ändamål med systemrisk alltid omfattas av de relevanta skyldigheterna enligt denna förordning. Definitionen bör inte omfatta AI-modeller som används innan de släpps ut på marknaden enbart för forsknings-, utvecklings- och prototypverksamhet. Detta påverkar inte skyldigheten att följa denna förordning när en modell släpps ut på marknaden efter sådan verksamhet.

(98) En modells generalitet kan, bland andra kriterier, också bestämmas av ett antal parametrar, men modeller med minst en miljard parametrar som tränats med en stor mängd data med hjälp av självövervakning i stor skala bör anses uppvisa betydande generalitet och på ett kompetent sätt utföra ett brett spektrum av olika uppgifter.

(99) Stora generativa AI-modeller är ett typiskt exempel på en AI-modell för allmänna ändamål, eftersom de möjliggör flexibel generering av innehåll (t.ex. i form av text, ljud, bilder eller video) som lätt kan rymma ett brett spektrum av olika uppgifter.

(100) När en AI-modell för allmänna ändamål integreras i eller ingår i ett AI-system bör detta system anses vara ett AI-system för allmänna ändamål när systemet, på grund av denna integrering, har förmåga att tjäna en rad olika ändamål. Ett AI-system för allmänna ändamål kan användas direkt eller integreras i andra AI-system.

(101) Leverantörer av AI-modeller för allmänna ändamål har en särskild roll och ett särskilt ansvar i AI-värdekedjan, eftersom de modeller som de tillhandahåller kan utgöra grunden för en rad system i efterföljande led, som ofta tillhandahålls av leverantörer i senare led, vilka behöver ha god kunskap om modellerna och deras kapacitet, både för att möjliggöra integrering av sådana modeller i sina produkter och för att fullgöra sina skyldigheter enligt denna eller andra förordningar. Därför bör proportionella transparensåtgärder föreskrivas, inbegripet utarbetande och uppdatering av dokumentation och tillhandahållande av information om AI-modellen för allmänna ändamål för dess användning av leverantörer i efterföljande led. Den tekniska dokumentationen bör utarbetas och hållas uppdaterad av leverantören av AI-modeller för allmänna ändamål så att den på begäran kan tillhandahållas AI-byrån och de nationella behöriga myndigheterna. Den minimiuppsättning element som ska ingå i sådan dokumentation bör anges i bilagorna till denna förordning. Kommissionen bör ges befogenhet att ändra dessa bilagor genom delegerade akter mot bakgrund av ny teknisk utveckling.

(102) Programvara och data, inbegripet modeller, som släpps ut med fri licens med öppen källkod som gör det möjligt att dela dem öppet och där användarna fritt kan få tillgång till, använda, modifiera och omdistribuera dem eller ändrade versioner av dem, kan bidra till forskning och innovation på marknaden och ge betydande tillväxtmöjligheter för unionens ekonomi. AI-modeller för allmänna ändamål som släpps ut med fri licens med öppen källkod bör övervägas för att säkerställa en hög grad av transparens och öppenhet om modellernas parametrar, inbegripet vikter, information om modellarkitekturen samt information om modellanvändning görs allmänt tillgängliga. Licensen bör betraktas som fri licens med öppen källkod även när den gör det möjligt för användare att köra, kopiera, distribuera, studera, ändra och förbättra programvara och data, inbegripet modeller under förutsättning att den ursprungliga leverantören av modellen krediteras och att identiska eller jämförbara distributionsvillkor respekteras.

(103) Fria AI-komponenter med öppen källkod omfattar programvara och data, inbegripet modeller och AI-modeller för allmänna ändamål, verktyg, tjänster eller processer i ett AI-system. Fria AI-komponenter med öppen källkod kan tillhandahållas genom olika kanaler, inbegripet deras utveckling i öppna databaser. Vid tillämpningen av denna förordning bör AI-komponenter som tillhandahålls mot en kostnad eller på annat sätt monetariseras, inbegripet genom tillhandahållande av tekniskt stöd eller andra tjänster, inbegripet genom en programvaruplattform, som rör AI-komponenten, eller användning av personuppgifter av andra skäl än uteslutande för att förbättra programvarans säkerhet, kompatibilitet eller interoperabilitet, med undantag för transaktioner mellan mikroföretag, inte omfattas av de undantag som föreskrivs för fria AI-komponenter med öppen källkod. Det faktum att AI-komponenter tillhandahålls via öppna databaser bör inte i sig utgöra en monetarisering.

(104) Leverantörer av AI-modeller för allmänna ändamål som släpps ut med en fri licens med öppen källkod och vars parametrar, inbegripet vikter, information om modellarkitekturen och information om modellanvändning, görs allmänt tillgängliga bör omfattas av undantag från de transparensrelaterade krav som gäller för AI-modeller för allmänna ändamål, såvida de inte kan anses utgöra en systemrisk, i vilket fall den omständigheten att modellen är transparent och åtföljs av en licens med öppen källkod inte bör anses vara ett tillräckligt skäl för att utesluta efterlevnad av skyldigheterna enligt denna förordning. Med tanke på att utsläppandet av AI-modeller för allmänna ändamål inom ramen för en fri licens med öppen källkod inte nödvändigtvis avslöjar väsentlig information om det dataset som används för träning eller finjustering av modellen och om hur efterlevnaden av upphovsrätten därmed säkerställdes, bör det undantag som föreskrivs för AI-modeller för allmänna ändamål från efterlevnad av transparensrelaterade krav under alla omständigheter inte avse skyldigheten att utarbeta en sammanfattning av det innehåll som används för modellträning och skyldigheten att införa en policy för efterlevnad av unionens upphovsrättsliga lagstiftning, särskilt för att identifiera och efterleva förbehållet för rättigheter i enlighet med artikel 4.3 i Europaparlamentets och rådets direktiv (EU) 2019/790[41].

[41] Europaparlamentets och rådets direktiv (EU) 2019/790 av den 17 april 2019 om upphovsrätt och närstående rättigheter på den digitala inre marknaden och om ändring av direktiven 96/9/EG och 2001/29/EG (EUT L 130, 17.5.2019, s. 92).

(105) Modeller för allmänna ändamål, särskilt stora generativa modeller, som kan generera text, bilder och annat innehåll, erbjuder unika innovationsmöjligheter men utgör även utmaningar för konstnärer, författare och andra upphovsmän och för det sätt på vilket deras kreativa innehåll skapas, distribueras, används och konsumeras. Utvecklingen och träningen av sådana modeller kräver tillgång till stora mängder text, bilder, videor och andra data. Text- och datautvinningstekniker kan användas i stor utsträckning i detta sammanhang för hämtning och analys av sådant innehåll, som kan vara skyddat av upphovsrätt och närstående rättigheter. All användning av upphovsrättsskyddat innehåll kräver tillstånd från den berörda rättsinnehavaren, såvida inte relevanta upphovsrättsliga undantag och inskränkningar tillämpas. Genom direktiv (EU) 2019/790 infördes undantag och inskränkningar som tillåter mångfaldigande av och utdrag ur verk eller andra alster, för text- och datautvinningsändamål, på vissa villkor. Enligt dessa regler får rättsinnehavare välja att rättigheterna till deras verk eller andra alster ska förbehållas dem för att förhindra text- och datautvinning, såvida detta inte sker för forskningsändamål. Om undantaget har förbehållits uttryckligen på lämpligt sätt måste leverantörer av AI-modeller för allmänna ändamål erhålla ett tillstånd från rättsinnehavarna om de vill utföra text- och datautvinning från sådana verk.

(106) Leverantörer som släpper ut AI-modeller för allmänna ändamål på unionsmarknaden bör säkerställa efterlevnad av de relevanta skyldigheterna i denna förordning. För detta ändamål bör leverantörer av AI-modeller för allmänna ändamål införa en policy för efterlevnad av unionsrätten om upphovsrätt och närstående rättigheter, särskilt för att identifiera och efterleva de förbehåll om rättigheter som uttryckts av rättsinnehavare i enlighet med artikel 4.3 i direktiv (EU) 2019/790. Alla leverantörer som släpper ut en AI-modell för allmänna ändamål på unionsmarknaden bör uppfylla denna skyldighet, oavsett i vilken jurisdiktion de upphovsrättsrelevanta handlingar som ligger till grund för träningen av dessa AI-modeller för allmänna ändamål äger rum. Detta är nödvändigt för att säkerställa lika villkor för leverantörer av AI-modeller för allmänna ändamål, så att ingen leverantör får en konkurrensfördel på unionsmarknaden genom att tillämpa lägre upphovsrättsstandarder än de som tillhandahålls i unionen.

(107) För att öka transparensen när det gäller de data som används i förträning och träning av AI-modeller för allmänna ändamål, inbegripet text och data som skyddas av upphovsrätt, är det lämpligt att leverantörer av sådana modeller utarbetar en tillräckligt detaljerad sammanfattning av det innehåll som används för att träna modellen för allmänna ändamål och gör denna allmänt tillgänglig. Samtidigt som vederbörlig hänsyn tas till behovet av att skydda företagshemligheter och konfidentiell affärsinformation bör denna sammanfattning ha en allmän omfattning med avseende på tillämpningsområde i stället för att vara tekniskt detaljerad, så att det blir det lättare för parter med legitima intressen, inbegripet upphovsrättsinnehavare, att utöva och hävda sina rättigheter enligt unionsrätten, till exempel genom att förteckna de viktigaste datauppsättningarna eller dataseten som ingick i träningen av modellen, såsom stora privata eller offentliga databaser eller dataarkiv, och genom att tillhandahålla en beskrivande förklaring om andra datakällor som använts. Det är lämpligt att AI-byrån tillhandahåller en mall för sammanfattningen, som bör vara enkel och effektiv och göra det möjligt för leverantören att tillhandahålla den begärda sammanfattningen i beskrivande form.

(108) När det gäller de skyldigheter som åläggs leverantörer av AI-modeller för allmänna ändamål att införa en policy för efterlevnad av unionens upphovsrättslagstiftning och göra en sammanfattning av det innehåll som används för träningen allmänt tillgänglig, bör AI-byrån övervaka huruvida leverantören har uppfyllt dessa skyldigheter utan att kontrollera eller gå vidare till en bedömning verk för verk av träningsdata när det gäller efterlevnaden av upphovsrätten. Denna förordning påverkar inte efterlevnaden av upphovsrättsliga bestämmelser enligt unionsrätten.

(109) Efterlevnaden av de skyldigheter som är tillämpliga på leverantörer av AI-modeller för allmänna ändamål bör stå i proportion till typen av modelleverantör, vilket utesluter behovet av efterlevnad för personer som utvecklar eller använder modeller för icke-yrkesmässiga ändamål eller vetenskapliga forskningsändamål, vilka dock bör uppmuntras att frivilligt uppfylla dessa krav. Utan att det påverkar tillämpningen av unionens upphovsrättslagstiftning bör fullgörandet av dessa skyldigheter ta vederbörlig hänsyn till leverantörens storlek och möjliggöra förenklade efterlevnadsmetoder för små och medelstora företag, inbegripet nystartade företag, som inte bör innebära en alltför stor kostnad och inte avskräcka från användningen av sådana modeller. Vid ändring eller finjustering av en modell bör leverantörernas skyldigheter begränsas till den ändringen eller finjusteringen, till exempel genom att komplettera den redan befintliga tekniska dokumentationen med information om ändringarna, inbegripet nya träningsdatakällor, som ett sätt att uppfylla de skyldigheter avseende värdekedjan som föreskrivs i denna förordning.

(110) AI-modeller för allmänna ändamål kan medföra systemrisker som omfattar, men inte är begränsade till, faktiska eller rimligen förutsebara negativa effekter i samband med allvarliga olyckor, störningar i kritiska sektorer och allvarliga konsekvenser för folkhälsan och säkerheten; alla faktiska eller rimligen förutsebara negativa effekter på demokratiska processer, allmän och ekonomisk säkerhet; spridning av olagligt, falskt eller diskriminerande innehåll. Det bör antas att systemrisker ökar med modellkapacitet och modellräckvidd, kan uppstå under modellens hela livscykel och påverkas av förhållanden med felaktig användning, modellens tillförlitlighet, rättvisa och säkerhet, dess grad av autonomi, tillgång till verktyg, nya eller kombinerade metoder, strategier för utsläppande och distribution, potentialen att avlägsna skyddsmekanismer och andra faktorer. I synnerhet har internationella strategier hittills identifierat behovet av att ägna uppmärksamhet åt risker till följd av potentiellt avsiktlig felaktig användning eller oavsiktliga kontrollproblem i samband med anpassning till mänsklig avsikt; kemiska, biologiska, radiologiska och nukleära risker, såsom de sätt på vilka inträdeshindren kan minskas, inbegripet för utveckling, konstruktion, förvärv eller användning av vapen; offensiv cyberkapacitet, såsom de sätt på vilka upptäckt, utnyttjande eller operativ användning av sårbarheter kan möjliggöras; effekterna av interaktion och verktygsanvändning, t.ex. kapaciteten att styra fysiska system och störa kritisk infrastruktur; risker med modeller för framställning kopior av dem själva eller ”självreplikering” eller träning av andra modeller; de sätt på vilka modeller kan ge upphov till skadlig snedvridning och diskriminering med risker för enskilda personer, grupper eller samhällen; underlättandet av desinformation eller skada på integritet med hot mot demokratiska värden och mänskliga rättigheter; risk för att en viss händelse kan leda till en kedjereaktion med betydande negativa effekter som kan påverka upp till en hel stad, en hel domäns verksamhet eller ett helt lokalsamhälle.

(111) En metod bör fastställas för klassificeringen av AI-modeller för allmänna ändamål som AI-modeller för allmänna ändamål med systemrisk. Eftersom systemrisker härrör från särskilt hög kapacitet bör en AI-modell för allmänna ändamål anses medföra systemrisker om den har kapacitet med hög påverkansgrad, utvärderad på grundval av lämpliga tekniska verktyg och metoder, eller har betydande inverkan på den inre marknaden på grund av sin räckvidd. Med kapacitet med hög påverkansgrad i AI-modeller för allmänna ändamål menas kapacitet som motsvarar eller överstiger den kapacitet som registrerats i de mest avancerade AI-modellerna för allmänna ändamål. Hela spektrumet av kapacitet i en modell kan förstås bättre efter det att den släppts ut på marknaden eller när användarna interagerar med modellen. Enligt teknikens ståndpunkt vid tidpunkten för denna förordnings ikraftträdande är den sammanlagda mängd beräkningskraft som används för träning av AI-modellen för allmänna ändamål, mätt i flyttalsberäkningar, en av de relevanta approximationerna för modellkapacitet. Den mängd beräkningskraft som används för träning kumulerar den beräkningskraft som används för de verksamheter och metoder som är avsedda att förbättra modellens kapacitet före införandet, såsom förträning, generering av syntetiska data och finjustering. Därför bör ett inledande tröskelvärde för flyttalsberäkningar fastställas som, om det uppfylls av en AI-modell för allmänna ändamål, leder till en presumtion om att modellen är en AI-modell för allmänna ändamål med systemrisker. Detta tröskelvärde bör justeras med tiden för att återspegla tekniska och industriella förändringar, såsom algoritmiska förbättringar eller ökad hårdvarueffektivitet, och bör kompletteras med riktmärken och indikatorer för modellkapacitet.

För att ta fram underlag för detta bör AI-byrån samarbeta med forskarsamhället, industrin, det civila samhället och andra experter. Tröskelvärden, liksom verktyg och riktmärken för bedömning av kapacitet med hög påverkansgrad, bör vara kraftfulla prediktorer för generalitet, dess kapacitet och tillhörande systemrisk hos AI-modeller för allmänna ändamål, och kan ta hänsyn till hur modellen kommer att släppas ut på marknaden eller hur många användare den kan påverka. För att komplettera detta system bör det finnas möjlighet för kommissionen att fatta enskilda beslut om att utse en AI-modell för allmänna ändamål till en AI-modell för allmänna ändamål med systemrisk, om det konstateras att en sådan modell har en kapacitet eller en inverkan som är likvärdig med den som blir resultatet med det fastställda tröskelvärdet. Det beslutet bör fattas på grundval av en övergripande bedömning av de kriterier för utseende av AI-modeller för allmänna ändamål med systemrisk som anges i en bilaga till denna förordning, såsom kvaliteten på eller storleken på träningsdatasetet, antalet företags- och slutanvändare, dess metoder för in- och utdata, dess grad av autonomi och skalbarhet, eller de verktyg som det har tillgång till. På motiverad begäran av en leverantör vars modell har betecknats som en AI-modell för allmänna ändamål med systemrisk bör kommissionen beakta begäran och kan besluta att ompröva huruvida AI-modellen för allmänna ändamål fortfarande kan anses medföra systemrisker.

(112) En metod bör fastställas för klassificeringen av AI-modeller för allmänna ändamål som AI-modeller för allmänna ändamål med systemrisk. En AI-modell för allmänna ändamål som uppfyller det tillämpliga tröskelvärdet för kapacitet med hög påverkansgrad bör antas vara en AI-modell för allmänna ändamål med systemrisk. Leverantören bör underrätta AI-byrån senast två veckor efter det att kraven har uppfyllts eller det blir känt att en AI-modell för allmänna ändamål kommer att uppfylla de krav som leder till presumtionen. Detta är särskilt relevant när det gäller tröskelvärdet för flyttalsberäkningar, eftersom träning av AI-modeller för allmänna ändamål kräver betydande planering, vilket inbegriper förhandstilldelning av beräkningskraftsresurser, och därför kan leverantörer av AI-modeller för allmänna ändamål veta om deras modell skulle uppfylla tröskelvärdet innan träningen avslutas. I samband med denna underrättelse bör leverantören kunna visa att en AI-modell för allmänna ändamål på grund av sina särskilda egenskaper undantagsvis inte medför några systemrisker och att den därför inte bör klassificeras som en AI-modell för allmänna ändamål med systemrisker. Denna information är värdefull för att AI-byrån ska kunna förutse utsläppandet på marknaden av AI-modeller för allmänna ändamål med systemrisker, och leverantörerna kan börja samarbeta med AI-byrån i ett tidigt skede. Informationen är särskilt viktig när det gäller AI-modeller för allmänna ändamål som planeras att släppas ut med öppen källkod, med tanke på att de åtgärder som krävs för att säkerställa efterlevnaden av skyldigheterna enligt denna förordning kan vara svårare att genomföra efter att modeller med öppen källkod har släppts ut.

(113) Om kommissionen får kännedom om att en AI-modell för allmänna ändamål uppfyller kraven för att klassificeras som en modell för allmänna ändamål med systemrisk, som antingen inte tidigare varit känd eller som den berörda leverantören inte har underrättat kommissionen om, bör kommissionen ges befogenhet att beteckna den som det. Ett system med kvalificerade varningar bör säkerställa att den vetenskapliga panelen uppmärksammar AI-byrån på AI-modeller för allmänna ändamål som eventuellt bör klassificeras som AI-modeller för allmänna ändamål med systemrisk, utöver AI-byråns övervakningsverksamhet.

(114) Utöver de skyldigheter som föreskrivs för leverantörer av AI-modeller för allmänna ändamål bör leverantörer av AI-modeller för allmänna ändamål som medför systemrisker omfattas av skyldigheter som syftar till att identifiera och begränsa dessa risker och säkerställa en lämplig nivå av cybersäkerhetsskydd, oavsett om den tillhandahålls som en fristående modell eller inbyggd i ett AI-system eller en produkt. För att uppnå dessa mål bör det i denna förordning krävas att leverantörer utför nödvändiga utvärderingar av modeller, särskilt innan de släpps ut på marknaden för första gången, vilket bör inbegripa att genomföra och dokumentera antagonistiska tester av modeller, även när så är lämpligt genom intern eller oberoende extern testning. Dessutom bör leverantörer av AI-modeller för allmänna ändamål med systemrisker kontinuerligt bedöma och begränsa systemriskerna, bland annat genom att införa riskhanteringspolicyer, såsom processer för ansvarsskyldighet och styrning, genomföra övervakning efter utsläppande på marknaden, vidta lämpliga åtgärder längs hela modellens livscykel och samarbeta med relevanta aktörer längs AI-värdekedjan.

(115) Leverantörer av AI-modeller för allmänna ändamål med systemrisker bör bedöma och begränsa eventuella systemrisker. Om utvecklingen eller användningen av modellen, trots insatser för att identifiera och förebygga risker i samband med en AI-modell för allmänna ändamål som kan medföra systemrisker, orsakar en allvarlig incident, bör leverantören av AI-modellen för allmänna ändamål utan onödigt dröjsmål bevaka incidenten och rapportera all relevant information och möjliga korrigerande åtgärder till kommissionen och de nationella behöriga myndigheterna. Dessutom bör leverantörerna säkerställa en lämplig nivå av cybersäkerhetsskydd för modellen och dess fysiska infrastruktur, om så är lämpligt, under modellens hela livscykel. Cybersäkerhetsskydd som avser systemrisker i samband med skadlig användning av eller attacker bör ta vederbörlig hänsyn till oavsiktligt modelläckage, otillåtet utsläppande, kringgående av säkerhetsåtgärder och försvar mot cyberattacker, obehörig åtkomst eller modellstöld. Detta skydd kan underlättas genom att man säkrar modellvikter, algoritmer, servrar och dataset, t.ex. genom operativa säkerhetsåtgärder för informationssäkerhet, särskilda cybersäkerhetspolicyer, lämpliga tekniska och etablerade lösningar samt kontroller av cyberåtkomst och fysisk åtkomst som är lämpliga för de relevanta omständigheterna och riskerna i samband med detta.

(116) AI-byrån bör uppmuntra och underlätta utarbetandet, översynen och anpassningen av förfarandekoder, med beaktande av internationella strategier. Alla leverantörer av AI-modeller för allmänna ändamål kan bjudas in att delta. För att säkerställa att förfarandekoderna återspeglar teknikens allmänt erkända ståndpunkt och tar vederbörlig hänsyn till en rad olika perspektiv bör AI-byrån samarbeta med relevanta nationella behöriga myndigheter och kan, när så är lämpligt, samråda med det civila samhällets organisationer och andra relevanta intressenter och experter, inbegripet den vetenskapliga panelen, för att utarbeta sådana koder. Förfarandekoder bör omfatta skyldigheter för leverantörer av AI-modeller för allmänna ändamål och modeller för allmänna ändamål som utgör systemrisker. När det gäller systemrisker bör förfarandekoder dessutom bidra till att fastställa en risktaxonomi för systemriskernas typ och art på unionsnivå, inbegripet källorna till dem. Förfarandekoder bör också inriktas på särskilda riskbedömnings- och riskbegränsningsåtgärder.

(117) Förfarandekoderna bör utgöra ett centralt verktyg för korrekt fullgörande av de skyldigheter som föreskrivs i denna förordning för leverantörer av AI-modeller för allmänna ändamål. Leverantörerna bör kunna förlita sig på förfarandekoder för att visa att skyldigheterna fullgörs. Genom genomförandeakter kan kommissionen besluta att godkänna en förfarandekod och ge den en allmän giltighet inom unionen, eller alternativt att tillhandahålla gemensamma regler för genomförandet av de relevanta skyldigheterna, om en förfarandekod vid den tidpunkt då denna förordning blir tillämplig inte kan färdigställas eller inte anses vara lämplig av AI-byrån. När en harmoniserad standard har offentliggjorts och bedömts vara lämplig för att täcka AI-byråns relevanta skyldigheter bör efterlevnaden av en europeisk harmoniserad standard ge leverantörerna presumtion om överensstämmelse. Leverantörer av AI-modeller för allmänna ändamål bör dessutom kunna påvisa efterlevnad med hjälp av alternativa lämpliga sätt, om förfarandekoder eller harmoniserade standarder inte finns tillgängliga, eller om de väljer att inte förlita sig på dessa.

(118) Denna förordning reglerar AI-system och AI-modeller genom att införa vissa krav och skyldigheter för relevanta marknadsaktörer som släpper ut dem på marknaden, tar dem i bruk eller använder dem i unionen, och kompletterar därigenom skyldigheterna för leverantörer av förmedlingstjänster som bygger in sådana system eller modeller i sina tjänster som regleras genom Europaparlamentets och rådets förordning (EU) 2022/2065[42]. I den mån sådana system eller modeller är inbyggda i utsedda mycket stora onlineplattformar eller mycket stora onlinesökmotorer omfattas de av den riskhanteringsram som föreskrivs i förordning (EU) 2022/2065. Följaktligen bör motsvarande skyldigheter i denna förordning förutsättas vara uppfyllda, såvida inte betydande systemrisker som inte omfattas av förordning (EU) 2022/2065 uppstår och identifieras i sådana modeller. Inom denna ram är leverantörer av mycket stora onlineplattformar och mycket stora onlinesökmotorer skyldiga att bedöma potentiella systemrisker som härrör från utformningen, funktionen och användningen av deras tjänster, inbegripet hur utformningen av algoritmiska system som används i tjänsten kan bidra till sådana risker, samt systemrisker som härrör från potentiell felaktig användning. Dessa leverantörer är också skyldiga att vidta lämpliga riskbegränsningsåtgärder med respekt för de grundläggande rättigheterna.

[42] Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster) (EUT L 277, 27.10.2022, s. 1).

(119) Med tanke på den snabba innovationstakten och den tekniska utvecklingen av digitala tjänster som omfattas av olika unionsrättsliga instrument, särskilt med tanke på mottagarnas användning och uppfattning, kan de AI-system som omfattas av denna förordning tillhandahållas som förmedlingstjänster eller delar av sådana i den mening som avses i förordning (EU) 2022/2065, som bör tolkas på ett teknikneutralt sätt. AI-system kan till exempel användas för att tillhandahålla onlinesökmotorer, särskilt i den mån ett AI-system såsom en onlinechatbot gör sökningar på, i princip, alla webbplatser, sedan införlivar resultaten i sin befintliga kunskap och använder den uppdaterade kunskapen för att generera ett enda resultat som kombinerar olika informationskällor.

(120) Dessutom är de skyldigheter som åläggs leverantörer och spridare av vissa AI-system i denna förordning för att det ska vara möjligt att upptäcka och visa att utdata från dessa system genereras eller manipuleras artificiellt vara särskilt relevanta för att underlätta ett effektivt genomförande av förordning (EU) 2022/2065. Detta gäller särskilt i fråga om skyldigheterna för leverantörer av mycket stora onlineplattformar eller mycket stora onlinesökmotorer att identifiera och begränsa systemrisker som kan uppstå till följd av spridning av innehåll som genererats eller manipulerats artificiellt, särskilt risken för faktiska eller förutsebara negativa effekter på demokratiska processer, samhällsdebatten och valprocesser, inbegripet genom desinformation.

(121) Standardisering bör ha en nyckelroll för att förse leverantörerna med tekniska lösningar för att säkerställa efterlevnaden av denna förordning ***i linje med teknikens ståndpunkt, för att främja innovation samt konkurrenskraft och tillväxt på den inre marknaden***. Överenstämmelse med harmoniserade standarder enligt definitionen i artikel 2.1 c i Europaparlamentets och rådets förordning (EU) nr 1025/2012[43], som normalt förväntas återspegla teknikens ståndpunkt bör vara ett sätt för leverantörerna att visa att de uppfyller kraven i denna förordning. ***En balanserad representation av intressen som involverar alla berörda parter i utarbetandet av standarder, särskilt små och medelstora företag, konsumentorganisationer samt miljö- och arbetstagarintressenter i enlighet med artiklarna 5 och 6 i förordning (EU) nr 1025/2012, bör därför uppmuntras. För att underlätta efterlevnaden bör begäranden om standardisering utfärdas av kommissionen utan onödigt dröjsmål. När kommissionen utarbetar en begäran om standardisering bör den samråda med det rådgivande forumet och nämnden för att samla in relevant expertis. I avsaknad av relevanta hänvisningar till harmoniserade standarder bör kommissionen*** dock***, genom genomförandeakter och efter samråd med det rådgivande forumet, kunna fastställa gemensamma specifikationer för vissa krav enligt denna förordning.***

[43] Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

Den gemensamma ***specifikationen bör vara en exceptionell reservlösning för att underlätta leverantörens skyldighet att uppfylla kraven i denna förordning, när begäran om standardisering inte har godtagits av någon av de europeiska standardiseringsorganisationerna eller när de relevanta harmoniserade standarderna inte i tillräcklig utsträckning behandlar frågor om grundläggande rättigheter, eller när de*** harmoniserade ***standarderna inte överensstämmer med begäran, eller när antagandet av en lämplig harmoniserad standard försenas***. ***Om en sådan försening av antagandet av en harmoniserad standard beror på den tekniska komplexiteten hos standarden i fråga bör kommissionen överväga detta innan man överväger att fastställa gemensamma specifikationer. Vid utarbetandet av gemensamma specifikationer uppmanas kommissionen att samarbeta med internationella partner och internationella standardiseringsorgan.***

(122) Utan att det påverkar användningen av harmoniserade standarder och gemensamma specifikationer är det lämpligt att leverantörer av AI-system med hög risk som har tränats och testats på data som återspeglar den specifika geografiska, beteendemässiga, kontextuella eller funktionella situation där AI-systemet är avsett att användas, förutsätts följa den relevanta åtgärd som föreskrivs i kravet på dataförvaltning i denna förordning. Utan att det påverkar de krav avseende robusthet och noggrannhet som fastställs i denna förordning, i enlighet med artikel 54.3 i Europaparlamentets och rådets förordning (EU) 2019/881[44], bör AI-system med hög risk som har certifierats eller för vilka en försäkran om överensstämmelse har utfärdats inom ramen för en cybersäkerhetsordning i enlighet med den förordningen och till vilka hänvisningar har offentliggjorts i Europeiska unionens officiella tidning förutsättas uppfylla cybersäkerhetskravet i den här förordningen i den mån cybersäkerhetscertifikatet eller försäkran om överensstämmelse eller delar därav omfattar cybersäkerhetskravet i denna förordning. Detta påverkar inte cybersäkerhetsordningens frivilliga karaktär.

(123) För att säkerställa en hög nivå av tillförlitlighet för AI-system med hög risk bör sådana system vara föremål för en bedömning av överensstämmelse innan de släpps ut på marknaden eller tas i bruk.

---

[44] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

(124) För att minimera bördan för operatörerna och förhindra allt eventuellt dubbelarbete är det, för AI-system med hög risk som är relaterade till produkter som omfattas av befintlig unionslagstiftning om harmonisering som bygger på den nya lagstiftningsramen, lämpligt att bedöma dessa AI-systems uppfyllande av kraven i denna förordning inom ramen för den bedömning av överensstämmelse som redan föreskrivs i den lagstiftningen. Tillämpligheten för kraven i denna förordning bör därmed inte påverka den specifika logiken, metoden eller allmänna strukturen för bedömningen av överensstämmelse i enlighet med den relevanta specifika unionslagstiftningen om harmonisering. ▌

(125) Med tanke på ***komplexiteten hos AI-system med hög risk och de risker som är förknippade med dem är det viktigt att utveckla ett lämpligt system för förfarandet för bedömning av överensstämmelse för AI-system med hög risk som involverar anmälda organ, så kallad tredjepartsbedömning av överensstämmelse***. ***Mot bakgrund av den nuvarande*** erfarenheten av professionella certifieringsorgan före utsläppandet på marknaden på området produktsäkerhet och de olika typer av risker som är involverade är det dock lämpligt att, åtminstone i den inledande fasen av denna förordnings tillämpning, begränsa tillämpningsområdet för tredjepartsbedömning av överensstämmelse när det gäller andra AI-system med hög risk än dem som är relaterade till produkter. Därför bör bedömningen av överensstämmelse för sådana system som en allmän regel utföras av leverantören på eget ansvar, med det enda undantaget för AI-system som är avsedda att användas för ***biometri***.

(126) För genomförandet av tredjeparts***bedömningar*** av överensstämmelse ***när så krävs***, bör anmälda organ ***anmälas*** inom ramen för denna förordning av de nationella behöriga myndigheterna, under förutsättning att de uppfyller ett antal krav, i synnerhet vad gäller oberoende, kompetens, avsaknad av intressekonflikter ***samt lämpliga krav för cybersäkerhet***. ***De nationella behöriga myndigheterna bör skicka anmälan av dessa organ till kommissionen och de övriga medlemsstaterna med hjälp av det elektroniska anmälningsverktyg som utvecklats och förvaltas av kommissionen i enlighet med artikel R23 i bilaga I till beslut nr 768/2008/EG.***

(127) I linje med unionens åtaganden enligt Världshandelsorganisationens avtal om tekniska handelshinder är det lämpligt att underlätta ömsesidigt erkännande av resultat av bedömningar av överensstämmelse som tagits fram av behöriga organ för bedömning av överensstämmelse som är oberoende av det territorium där de är etablerade, förutsatt att dessa organ för bedömning av överensstämmelse som inrättats enligt lagstiftningen i ett tredjeland uppfyller de tillämpliga kraven i denna förordning och att unionen har ingått ett avtal om detta. I detta sammanhang bör kommissionen aktivt undersöka möjliga internationella instrument för detta ändamål och särskilt sträva efter att ingå avtal om ömsesidigt erkännande med tredjeländer.

(128) Vid varje ändring som kan påverka efterlevnaden av denna förordning för ***ett AI***-system ***med hög risk (t.ex. en ändring av operativsystem eller programvaruarkitektur)*** eller vid ändring av systemets avsedda ändamål är det lämpligt ***att*** ▌ ***AI-systemet***, i linje med det vedertagna begreppet väsentlig ändring som avser produkter som regleras genom unionens harmoniseringslagstiftning ***anses vara ett nytt AI-system som bör genomgå en ny bedömning av överensstämmelse***. ***Ändringar av algoritmen och prestandan i*** AI-system som fortsätter sin ”inlärning” efter att de släppts ut på marknaden eller tagits i bruk, dvs. ▌ automatiskt ***anpassar*** hur funktionerna utförs, ***bör dock inte utgöra väsentliga ändringar, förutsatt att dessa ändringar*** på förhand har fastställts av leverantören och bedömts vid tidpunkten för bedömning av överensstämmelse ▌ .

(129) AI-system med hög risk bör vara försedda med en CE-märkning som visar att de överensstämmer med denna förordning, så att de kan omfattas av den fria rörligheten på den inre marknaden. ***För AI-system med hög risk som är inbyggda i en produkt bör en fysisk CE-märkning anbringas, och den kan kompletteras med en digital CE-märkning. För AI-system med hög risk som endast tillhandahålls digitalt bör en digital CE-märkning användas.*** Medlemsstaterna bör inte sätta upp omotiverade hinder för utsläppandet på marknaden eller ibruktagandet av AI-system med hög risk som uppfyller kraven i denna förordning och är försedda med en CE-märkning.

(130) Under vissa omständigheter kan en snabb tillgång till innovativ teknik vara avgörande för hälsan och säkerheten för personer, ***miljöskyddet och klimatförändringarna*** och för samhället som helhet. Det är därför lämpligt att ***marknadskontrollmyndigheterna***, när det föreligger exceptionella skäl som rör ***allmän säkerhet*** eller skydd av fysiska personers liv och hälsa, ***miljöskydd*** och skydd av ***viktiga industriella och infrastrukturella tillgångar,*** har möjlighet att tillåta utsläppandet på marknaden eller ibruktagandet av AI-system som inte har genomgått en bedömning av överensstämmelse. ***I en vederbörligen motiverad situation enligt denna förordning kan brottsbekämpande myndigheter eller civilskyddsmyndigheter ta ett specifikt AI-system med hög risk i bruk utan marknadskontrollmyndighetens tillstånd, förutsatt att ett sådant tillstånd begärs under eller efter användningen utan onödigt dröjsmål.***

(131) För att underlätta kommissionens och medlemsstaternas arbete på AI-området och öka transparensen gentemot allmänheten, bör leverantörer av andra AI-system med hög risk än dem som är relaterade till produkter som faller inom tillämpningsområdet för relevant befintlig unionslagstiftning om harmonisering***, samt leverantörer som anser att AI-systemet med hög risk som är förtecknat i en bilaga till denna förordning inte är ett AI-system med hög risk på grundval av ett undantag,*** åläggas att registrera ***sig själva och information om sina*** AI-system i en EU-databas som ska upprättas och förvaltas av kommissionen. ***Innan ett sådant AI-system med hög risk används bör spridare av AI-system med hög risk som är offentliga myndigheter, byråer eller organ registrera sig i en sådan databas och välja det system som de avser att använda.***

Andra spridare bör ha rätt att göra detta frivilligt. Denna del av databasen bör vara kostnadsfritt åtkomlig för allmänheten, och det bör vara lätt att navigera i informationen, som bör vara begriplig och maskinläsbar. Databasen bör också vara användarvänlig, till exempel genom att sökfunktioner, inbegripet genom nyckelord, tillhandahålls som gör det möjligt för allmänheten att hitta relevant information som ska lämnas in vid registreringen av AI-system med hög risk och om de AI-system med hög risk som anges i bilagor till denna förordning och som AI-systemen med hög risk motsvarar. Alla väsentliga ändringar av AI-system med hög risk bör också registreras i EU-databasen. För AI-system med hög risk på området brottsbekämpning, migration, asyl och gränskontrollförvaltning bör registreringsskyldigheterna uppfyllas i en säker icke-offentlig del av databasen. Åtkomsten till den säkra icke-offentliga delen bör strikt begränsas till kommissionen och till marknadskontrollmyndigheterna när det gäller deras nationella del av databasen. AI-system med hög risk på området kritisk infrastruktur bör endast registreras på nationell nivå. Kommissionen bör vara personuppgiftsansvarig för ***EU-***databas***en*** i enlighet med förordning (EU) 2018/1725. För att säkerställa att databasen är fullt funktionell när den börjar utnyttjas, bör förfarandet för inrättandet av databasen innefatta funktionsspecifikationer som utarbetas av kommissionen samt en oberoende revisionsrapport. ***Kommissionen bör ta hänsyn till risker som rör cybersäkerhet och fara när den utför sina uppgifter som personuppgiftsansvarig i EU-databasen. För att allmänheten ska få så stor tillgång till och kunna använda databasen så mycket som möjligt bör databasen, och den information som tillgängliggörs genom den, uppfylla kraven i direktiv (EU) 2019/882.***

(132) Vissa AI-system avsedda för att interagera med fysiska personer eller generera innehåll kan utgöra särskilda risker för identitetsmissbruk eller vilseledning oavsett om de kategoriseras som hög risk eller inte. Under vissa omständigheter bör därför användningen av dessa system omfattas av särskilda transparensskyldigheter utan att det påverkar kraven eller skyldigheterna för AI-system med hög risk ***och omfattas av riktade undantag för att ta hänsyn till brottsbekämpningens särskilda behov***. I synnerhet bör fysiska personer underrättas om att de interagerar med ett AI-system, såvida detta inte är uppenbart ***för en fysisk person som är normalt informerad och skäligen uppmärksam och medveten med beaktande av*** omständigheterna kring och sammanhanget för användningen. ***Vid genomförandet av en sådan skyldighet bör det som kännetecknar enskilda personer som tillhör grupper av sårbara personer på grund av ålder eller funktionsnedsättning beaktas i den mån AI-systemet även är avsett att interagera med dessa grupper. Dessutom bör fysiska personer underrättas när de utsätts för system som genom att behandla deras biometriska uppgifter kan identifiera eller härleda dessa personers känslor eller avsikter eller hänföra dem till särskilda kategorier. Sådana särskilda kategorier kan avse aspekter som kön, ålder, hårfärg, ögonfärg, tatueringar, personlighetsdrag, etniskt ursprung, personliga preferenser och intressen. Sådan information och sådana underrättelser bör tillhandahållas i format som är tillgängliga för personer med funktionsnedsättning.***

(133) En rad olika AI-system kan generera stora mängder syntetiskt innehåll som blir allt svårare för människor att skilja från mänskligt genererat och autentiskt innehåll. Dessa systems breda tillgänglighet och ökande kapacitet har en betydande inverkan på integriteten och förtroendet för informationsekosystemet, vilket medför nya risker för felaktig information och manipulering i stor skala, bedrägeri, identitetsmissbruk och vilseledande av konsumenter. Mot bakgrund av denna inverkan, den snabba tekniska takten och behovet av nya metoder och tekniker för att spåra ursprunget till information är det lämpligt att kräva att leverantörer av dessa system integrerar tekniska lösningar som möjliggör märkning i maskinläsbart format och upptäckt av att utdata har genererats eller manipulerats av ett AI-system och inte av en människa. Sådana tekniker och metoder bör vara tillräckligt tillförlitliga, driftskompatibla, effektiva och robusta i den mån det är tekniskt möjligt, med beaktande av tillgänglig teknik eller en kombination av sådana tekniker, såsom vattenmärken, metadataidentifiering, krypteringsmetoder för att bevisa innehållets härkomst och äkthet, loggningsmetoder, fingeravtryck eller annan teknik, beroende på vad som är lämpligt. När denna skyldighet fullgörs bör leverantörer även beakta särdragen och begränsningarna hos olika typer av innehåll, och den relevanta tekniska utvecklingen och marknadsutvecklingen på området, såsom detta återspeglas i den allmänt erkända tidigare kända tekniken. Sådana tekniker och metoder kan genomföras på systemnivå eller modellnivå, inbegripet i fråga om AI-modeller för allmänna ändamål som genererar innehåll, för att därigenom underlätta fullgörandet av denna skyldighet av AI-systemets leverantör i efterföljande led. För att förbli proportionerlig är det lämpligt att föreskriva att denna märkningsskyldighet inte bör omfatta AI-system som i första hand utför en hjälpfunktion för vanlig redigering eller AI-system som inte väsentligt ändrar de indata som tillhandahålls av spridaren eller deras semantik.

(134) Med hänsyn till de tekniska lösningar som används av systemleverantörerna bör spridare som använder ett AI-system för att generera eller manipulera bilder eller ljud- eller videoinnehåll som på ett märkbart sätt liknar befintliga personer, platser eller händelser, och som för en person felaktigt kan framstå som autentiska (deepfake), även på ett tydligt och urskiljbart sätt upplysa om att innehållet har skapats artificiellt eller manipulerats genom märkning av de utdata som producerats med artificiell intelligens i enlighet med det och upplysa om dess artificiella ursprung. Fullgörandet av denna transparensskyldighet bör inte tolkas som att användningen av systemet eller dess utdata hindrar rätten till yttrandefrihet och konstens och vetenskapens frihet, som garanteras i stadgan, särskilt när innehållet ingår i ett uppenbart kreativt, satiriskt, konstnärligt eller skönlitterärt verk eller program, med förbehåll för lämpliga garantier för tredje mans rättigheter och friheter. I dessa fall är den transparensskyldighet för deepfake som fastställs i denna förordning begränsad till en upplysning om förekomsten av sådant genererat eller manipulerat innehåll på ett lämpligt sätt som inte hindrar visningen eller åtnjutandet av verket, inbegripet dess normala utnyttjande och användning, samtidigt som verkets nytta och kvalitet upprätthålls. Det är också lämpligt att föreskriva en liknande upplysningsskyldighet när det gäller AI-genererad eller AI-manipulerad text i den mån den offentliggörs i syfte att informera allmänheten om frågor av allmänt intresse, såvida inte det AI-genererade innehållet har genomgått en process för mänsklig granskning eller redaktionell kontroll och en fysisk eller juridisk person har redaktionellt ansvar för offentliggörandet av innehållet.

(135) För att säkerställa ett konsekvent genomförande är det lämpligt att ge kommissionen befogenhet att anta genomförandeakter om tillämpningen av bestämmelserna om märkning och upptäckt av artificiellt genererat eller manipulerat innehåll. Utan att det påverkar transparensskyldigheternas obligatoriska karaktär och fullständiga tillämplighet kan kommissionen också uppmuntra och underlätta utarbetandet av förfarandekoder på unionsnivå för att underlätta ett effektivt genomförande av skyldigheterna avseende upptäckt och märkning av artificiellt genererat eller manipulerat innehåll, bland annat för att stödja praktiska arrangemang för att, när så är lämpligt, göra mekanismerna för upptäckt tillgängliga och underlätta samarbetet med andra aktörer längs värdekedjan, sprida innehåll eller kontrollera dess autenticitet och ursprung för att göra det möjligt för allmänheten att på ett effektivt sätt urskilja AI-genererat innehåll.

(136) Dessutom är de skyldigheter som åläggs leverantörer och spridare av vissa AI-system i denna förordning för att det ska vara möjligt att upptäcka och visa att utdata från dessa system är artificiellt genererade eller manipulerade vara särskilt relevanta för att underlätta ett effektivt genomförande av förordning (EU) 2022/2065. Detta gäller särskilt i fråga om skyldigheterna för leverantörer av mycket stora onlineplattformar eller mycket stora onlinesökmotorer att identifiera och begränsa systemrisker som kan uppstå till följd av spridning av innehåll som genererats eller manipulerats artificiellt, särskilt risken för faktiska eller förutsebara negativa effekter på demokratiska processer, samhällsdebatten och valprocesser, inbegripet genom desinformation. Kravet på märkning av innehåll som genereras av AI-system enligt denna förordning påverkar inte skyldigheten i artikel 16.6 i förordning (EU) 2022/2065 för leverantörer av värdtjänster att behandla anmälningar om olagligt innehåll som mottagits i enlighet med artikel 16.1 i den förordningen och bör inte påverka bedömningen och beslutet om det specifika innehållets olaglighet. Denna bedömning bör göras endast med hänsyn till de regler som reglerar innehållets lagenlighet.

(137) Fullgörandet av transparensskyldigheterna för AI-system som omfattas av denna förordning bör inte tolkas som att användningen av systemet eller dess utdata är laglig enligt denna förordning eller annan unions- och medlemsstatslagstiftning och bör inte påverka andra transparensskyldigheter för spridare av AI-system som fastställs i unionsrätten eller nationell rätt.

(138) AI är en teknikfamilj i snabb utveckling som kräver tillsyn och ett säkert ***och kontrollerat*** område för experiment, med säkerställande av ansvarsfull innovation och integrering av ändamålsenliga skydds- och riskbegränsningsåtgärder. För att säkerställa en rättslig ram som ***främjar innovation och är*** framtidssäkrad och resilient mot störningar, ***bör medlemsstaterna säkerställa att deras nationella behöriga myndigheter inrättar åtminstone en*** regulatorisk sandlåda för AI ***på nationell nivå***, för att underlätta utveckling och testning av innovativa AI-system under strikt tillsyn innan dessa system släpps ut på marknaden eller på annat sätt tas i bruk. ***Medlemsstaterna kan också fullgöra denna skyldighet genom att delta i redan befintliga regulatoriska sandlådor eller gemensamt inrätta en sandlåda med en eller flera medlemsstaters behöriga myndigheter, i den mån detta deltagande ger de deltagande medlemsstaterna likvärdig nationell täckning. Regulatoriska sandlådor kan inrättas i fysisk eller digital form eller i hybridform och kan rymma både fysiska och digitala produkter. Inrättandet av myndigheter bör också säkerställa att de regulatoriska sandlådorna har tillräckliga resurser för sin funktion, inbegripet ekonomiska och mänskliga resurser.***

(139) Målen med dessa regulatoriska sandlådor ***för AI*** bör vara att främja AI-innovation genom inrättande av en kontrollerad experiment- och testmiljö vid utveckling och under fasen före utsläppandet på marknaden, med sikte på att säkerställa att de innovativa AI-systemen är förenliga med denna förordning och annan relevant unionsrätt och nationell rätt***,*** att öka rättssäkerheten för innovatörer och förbättra de behöriga myndigheternas tillsyn och förståelse av möjligheterna, de nya riskerna och effekterna av AI-användning, ***att underlätta regulatoriskt lärande för myndigheter och företag, även med tanke på framtida anpassningar av den rättsliga ramen, att stödja samarbete och utbyte av bästa praxis med de myndigheter som deltar i regulatoriska sandlådan för AI*** och att påskynda tillträdet till marknader, bland annat genom att undanröja hinder för små och medelstora företag***, inbegripet*** nystartade företag. ***Regulatoriska sandlådor bör vara tillgängliga i bred omfattning i hela unionen, och särskild uppmärksamhet bör ägnas åt deras tillgänglighet för små och medelstora företag, inbegripet nystartade företag. Deltagandet i den*** regulatoriska ***sandlådan för AI bör inriktas på problem som skapar rättsosäkerhet för leverantörer och potentiella leverantörer när de ska vara innovativa, experimentera med AI i unionen och bidra till evidensbaserat regulatoriskt lärande.*** Tillsynen av ***AI-systemen i den regulatoriska sandlådan för AI*** bör ***därför omfatta deras utveckling, träning, testning och validering innan systemen släpps ut på marknaden eller tas i bruk, samt begreppet och förekomsten av väsentlig ändring som kan kräva ett nytt förfarande för bedömning av överensstämmelse. Alla betydande risker som upptäcks under utvecklingen och testningen av sådana*** AI-system ***bör leda till omedelbar riskbegränsning och, om detta inte är möjligt, leda*** till att ***utvecklings- och testningsprocessen tillfälligt avbryts***.

När så är lämpligt bör nationella behöriga myndigheter som inrättar regulatoriska ***sandlådor*** för AI ***samarbeta med andra relevanta myndigheter, inbegripet dem som övervakar skyddet av de grundläggande rättigheterna, och de skulle kunna tillåta deltagande av andra aktörer inom AI-ekosystemet, såsom nationella eller europeiska standardiseringsorganisationer, anmälda organ, test- och experimentanläggningar, forsknings- och experimentlaboratorier, europeiska digitala innovationsknutpunkter och relevanta organisationer för berörda parter och för det civila samhället. För att säkerställa ett enhetligt genomförande i hela unionen och stordriftsfördelar är det*** lämpligt ***att fastställa gemensamma regler för införandet av regulatoriska sandlådor och en samarbetsram för de berörda*** myndigheter ***som deltar i tillsynen över sådana sandlådor. Regulatoriska sandlådor för AI som inrättas enligt denna förordning bör inte påverka annan lagstiftning som tillåter inrättande av andra sandlådor som syftar till att säkerställa överensstämmelse med annan unionslagstiftning än denna förordning. I lämpliga fall bör relevanta behöriga myndigheter som ansvarar för dessa andra regulatoriska sandlådor överväga fördelarna med att använda dessa sandlådor även i syfte att säkerställa AI-systemens överensstämmelse med denna förordning. Efter överenskommelse mellan de nationella*** behöriga myndigheterna ***och deltagarna i den regulatoriska sandlådan för AI kan testning under verkliga förhållanden också genomföras och övervakas inom ramen för den regulatoriska sandlådan för AI***.

(140) Denna förordning bör erbjuda den rättsliga grunden för att leverantörer och potentiella leverantörer i den regulatoriska sandlådan för AI använder personuppgifter som samlats in för andra ändamål för att utveckla vissa AI-system i allmänhetens intresse inom regulatoriska sandlådor för AI, endast på de angivna villkoren, i enlighet med artiklarna 6.4 och 9.2 g i förordning (EU) 2016/679 och artiklarna 5, 6 och 10 i förordning (EU) 2018/1725, och utan att det påverkar tillämpningen av artiklarna 4.2 och 10 i direktiv (EU) 2016/680. Alla andra skyldigheter för personuppgiftsansvariga och de registrerades rättigheter enligt förordningarna (EU) 2016/679 och (EU) 2018/1725 och direktiv (EU) 2016/680 förblir tillämpliga. I synnerhet bör denna förordning inte utgöra en rättslig grund i den mening som avses i artikel 22.2 b i förordning (EU) 2016/679 och artikel 24.2 b i förordning (EU) 2018/1725. Leverantörer och potentiella leverantörer i sandlådan bör säkerställa ändamålsenliga skyddsåtgärder och samarbeta med de behöriga myndigheterna, vilket omfattar att följa deras vägledning och agera snabbt och i god tro för att på lämpligt sätt begränsa eventuella identifierade väsentliga risker för säkerhet, hälsa och grundläggande rättigheter som kan uppstå i samband med utvecklings-, testnings- och experimentverksamhet i sandlådan.

(141) För att påskynda utvecklingen och utsläppandet på marknaden av de AI-system med hög risk som förtecknas i en bilaga till denna förordning är det viktigt att leverantörer eller potentiella leverantörer av sådana system också kan dra nytta av en särskild ordning för testning av dessa system under verkliga förhållanden, utan att delta i en regulatorisk sandlåda för AI. I sådana fall och med beaktande av de möjliga konsekvenserna av sådan testning för enskilda personer bör det dock säkerställas att lämpliga och tillräckliga garantier och villkor införs genom denna förordning för leverantörer eller potentiella leverantörer. Sådana garantier bör bland annat inbegripa en begäran om informerat samtycke från fysiska personer att delta i testning under verkliga förhållanden, med undantag för brottsbekämpning om inhämtandet av informerat samtycke skulle hindra AI-systemet från att testas. Försökspersonernas samtycke till att delta i sådan testning enligt denna förordning skiljer sig från och påverkar inte de registrerades samtycke till behandling av deras personuppgifter enligt relevant dataskyddslagstiftning.

Det är också viktigt att minimera riskerna och göra det möjligt för behöriga myndigheter att utöva tillsyn, och därför kräva att potentiella leverantörer har en plan för testning under verkliga förhållanden som lämnas in till den behöriga marknadskontrollmyndigheten och att de registrerar testningen i särskilda delar av EU-databasen med vissa begränsade undantag, samt att fastställa begränsningar för den period under vilken testningen kan utföras och kräva ytterligare skyddsåtgärder för utsatta personer, inbegripet grupper av utsatta personer, liksom ett skriftligt avtal där man definierar rollerna och ansvarsområdena för potentiella leverantörer och spridare samt formerna för en effektiv tillsyn av personal med lämplig kompetens som deltar i testningen under verkliga förhållanden. Det är dessutom lämpligt att överväga ytterligare skyddsåtgärder för att säkerställa att AI-systemets förutsägelser, rekommendationer eller beslut effektivt kan upphävas och ignoreras och att personuppgifter skyddas och raderas när försökspersonerna har dragit tillbaka sitt samtycke till att delta i testningen, utan att det påverkar deras rättigheter som registrerade enligt unionens dataskyddslagstiftning. När det gäller överföring av uppgifter är det också lämpligt att förutse att uppgifter som samlats in och behandlats för testning under verkliga förhållanden bör överföras till tredjeländer endast om lämpliga och tillämpliga skyddsåtgärder enligt unionsrätten vidtas, särskilt i enlighet med grunderna för överföring av personuppgifter enligt unionsrätten om dataskydd, medan det i fråga om icke-personuppgifter införs lämpliga skyddsåtgärder i enlighet med unionsrätten, såsom Europaparlamentets och rådets förordningar (EU) 2022/868[45] ***och*** (EU) 2023/2854[46]***.***

[45] Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten) (EUT L 152, 3.6.2022, s. 1).

[46] Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen) (EUT L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

(142) För att säkerställa att AI leder till socialt och miljömässigt fördelaktiga utfall uppmuntras medlemsstaterna att stödja och främja forskning och utveckling av AI-lösningar till stöd för socialt och miljömässigt fördelaktiga utfall, såsom AI-baserade lösningar för att öka tillgängligheten för personer med funktionsnedsättning, ta itu med socioekonomiska ojämlikheter eller uppnå miljömål, genom att anslå tillräckliga resurser, inbegripet offentlig finansiering och unionsfinansiering, och, när så är lämpligt och förutsatt att behörighets- och urvalskriterierna är uppfyllda, genom att särskilt beakta projekt som eftersträvar sådana mål. Projekten bör grunda sig på principen om interdisciplinärt samarbete mellan AI-utvecklare, experter på ojämlikhet och icke-diskriminering, tillgänglighet, konsument- och miljörättigheter samt digitala rättigheter, och akademiker.

(143) För att främja och skydda innovation är det viktigt att särskild hänsyn tas till intressena hos ***små och medelstora företag, inbegripet nystartade företag, som är leverantörer eller spridare*** av AI-system. I detta syfte bör medlemsstaterna ta fram initiativ som riktar sig till dessa operatörer, bland annat vad gäller medvetandehöjande och information. ***Medlemsstaterna bör ge små och medelstora företag, inbegripet nystartade företag, som har ett säte eller en filial i unionen prioriterad åtkomst till de regulatoriska sandlådorna för AI, förutsatt att de uppfyller behörighetskraven och urvalskriterierna och utan att andra leverantörer och potentiella leverantörer hindras från att få åtkomst till sandlådorna, förutsatt att samma krav och kriterier är uppfyllda. Medlemsstaterna bör använda befintliga kanaler och, när så är lämpligt, inrätta nya särskilda kanaler för kommunikation med små och medelstora företag, nystartade företag, spridare och andra innovatörer och, i förekommande fall, lokala offentliga myndigheter i syfte att stödja små och medelstora företag under deras utveckling genom att ge vägledning och svara på frågor om genomförandet av denna förordning. Där så är lämpligt bör dessa kanaler samarbeta för att skapa synergier och säkerställa homogenitet i sin vägledning till små och medelstora företag, inbegripet nystartade företag, och spridare. Medlemsstaterna bör dessutom underlätta små och medelstora företags och andra berörda parters deltagande i processerna för standardiseringsutveckling.*** De särskilda intressena och behoven hos ***små och medelstora företag, inbegripet nystartade företag,*** som är leverantörer ***bör*** också beaktas när de anmälda organen fastställer avgifterna för bedömning av överensstämmelse. ***Kommissionen bör regelbundet bedöma kostnaderna för certifiering och efterlevnad för små och medelstora företag, inbegripet nystartade företag, genom transparenta samråd med spridare, samt samarbeta med medlemsstaterna för att sänka sådana kostnader.***

Till exempel kan kostnaderna för översättning av obligatorisk dokumentation och kommunikation med myndigheter utgöra betydande kostnader för leverantörer och andra operatörer, i synnerhet mer småskaliga sådana. Medlemsstaterna bör eventuellt säkerställa att ett av de språk som fastställs och godtas av dem för relevant dokumentation från leverantörer och för kommunikation med operatörer är ett språk som i huvudsak förstås av största möjliga antal ***spridare*** i gränsöverskridande situationer. ***För att tillgodose de särskilda behoven hos små och medelstora företag, inbegripet nystartade företag, bör kommissionen på nämndens begäran tillhandahålla standardiserade mallar för de områden som omfattas av denna förordning. Kommissionen bör dessutom komplettera medlemsstaternas insatser genom att tillhandahålla en enda informationsplattform med information om denna förordning som är lätt att använda för alla leverantörer och spridare, genom att anordna lämpliga kommunikationskampanjer i syfte att öka medvetenheten om de skyldigheter som följer av denna förordning och genom att utvärdera och främja konvergens av bästa praxis i förfaranden för offentlig upphandling när det gäller AI-system. Medelstora företag som nyligen var små företag i den mening som avses i bilagan till kommissionens rekommendation 2003/361/EG[47] bör ha tillgång till dessa stödåtgärder, eftersom dessa nya medelstora företag ibland saknar de rättsliga resurser och den utbildning som krävs för att säkerställa en korrekt förståelse och efterlevnad av denna förordning***.

[47] Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

(144) För att främja och skydda innovation bör plattformen för efterfrågestyrd AI samt alla relevanta unionsfinansieringsprogram och unionsprojekt, såsom programmet för ett digitalt Europa och Horisont Europa, som genomförs av kommissionen och medlemsstaterna på unionsnivå eller nationell nivå i förekommande fall bidra till att målen i denna förordning uppnås.

(145) För att minimera risker för genomförandet som följer av bristande kunskap och expertis på marknaden, och för att främja leverantörernas, ***särskilt små och medelstora företags, inbegripet nystartade företags,*** och de anmälda organens uppfyllande av sina skyldigheter enligt denna förordning, bör plattformen för efterfrågestyrd AI, de europeiska digitala innovationsknutpunkterna och de test- och experimentanläggningar som inrättas av kommissionen och medlemsstaterna på unionsnivå eller nationell nivå ***i synnerhet*** bidra till genomförandet av denna förordning. Inom sina respektive uppdrag och kompetensområden kan plattformen för efterfrågestyrd AI, de europeiska digitala innovationsknutpunkterna och test- och experimentanläggningarna i synnerhet tillhandahålla tekniskt och vetenskapligt stöd till leverantörer och anmälda organ.

(146) Med tanke på vissa operatörers mycket begränsade storlek och för att säkerställa proportionalitet när det gäller innovationskostnader, bör dessutom mikroföretag tillåtas att fullgöra en av de mest kostsamma skyldigheterna, nämligen inrättandet av ett kvalitetsstyrningssystem, på ett förenklat sätt som skulle minska den administrativa bördan och kostnaderna för dessa företag utan att skyddsnivån och behovet av efterlevnad av kraven för AI-system med hög risk påverkas. Kommissionen bör utarbeta riktlinjer för att specificera de delar av kvalitetsstyrningssystemet som mikroföretagen bör fullgöra på detta förenklade sätt.

(147) Det är lämpligt att kommissionen i möjligaste mån underlättar tillgången till test- och experimentanläggningar för organ, grupper eller laboratorier som inrättats eller ackrediterats i enlighet med relevant unionslagstiftning om harmonisering och som utför uppgifter inom ramen för bedömning av överensstämmelse för produkter eller utrustning som omfattas av denna unionslagstiftning om harmonisering. Detta gäller i synnerhet för expertpaneler, expertlaboratorier och referenslaboratorier på området medicintekniska produkter i enlighet med förordningarna (EU) 2017/745 och (EU) 2017/746.

(148) Denna förordning bör fastställa en styrningsram som gör det möjligt såväl att samordna och stödja tillämpningen av denna förordning på nationell nivå som att bygga upp kapacitet på unionsnivå och involvera berörda parter på AI-området. Ett effektivt genomförande och en effektiv kontroll av efterlevnaden av denna förordning kräver en styrningsram som gör det möjligt att samordna och bygga upp central expertis på unionsnivå. AI-byrån inrättades genom ett kommissionsbeslut[48] och har som uppdrag att utveckla unionens expertis och kapacitet på AI-området och att bidra till genomförandet av unionsrätten om AI. Medlemsstaterna bör underlätta AI-byråns uppgifter med målet att stödja utvecklingen av unionens expertis och kapacitet på unionsnivå och stärka den digitala inre marknadens funktion. Det bör dessutom inrättas en nämnd bestående av företrädare för medlemsstaterna, en vetenskaplig panel för att involvera forskarsamhället och ett rådgivande forum för att genom synpunkter från berörda parter bidra till genomförandet av denna förordning, på unionsnivå och nationell nivå. Utvecklingen av unionens expertis och kapacitet bör också inbegripa användning av befintliga resurser och befintlig expertis, särskilt genom synergier med strukturer som byggts upp i samband med efterlevnaden av annan lagstiftning på unionsnivå och synergier med därmed sammanhängande initiativ på unionsnivå, såsom det gemensamma företaget EuroHPC och test- och experimentanläggningar för AI inom ramen för programmet för ett digitalt Europa.

[48] Kommissionens beslut av den 24 januari 2024 om inrättande av Europeiska byrån för artificiell intelligens C(2024) 390.

(149) För att främja ett smidigt, effektivt och harmoniserat genomförande av denna förordning bör en nämnd inrättas. Nämnden bör ***återspegla AI-ekosystemets olika intressen och bestå av företrädare för medlemsstaterna. Nämnden bör*** ansvara för ett antal rådgivande uppgifter, däribland att utfärda yttranden, rekommendationer, råd eller ***bidra till*** vägledning om frågor som rör genomförandet av denna förordning, inbegripet när det gäller ***frågor som rör kontroll av efterlevnad,*** tekniska specifikationer eller befintliga standarder avseende kraven i denna förordning och råd till ***kommissionen, medlemsstaterna och deras nationella behöriga myndigheter*** om specifika frågor som rör AI. ***För att ge medlemsstaterna viss flexibilitet när de utser sina företrädare i nämnden kan sådana företrädare utgöras av alla personer som tillhör offentliga enheter och som bör ha relevant kompetens och relevanta befogenheter för att underlätta samordningen på nationell nivå och bidra till att nämndens uppgifter fullgörs. Nämnden bör inrätta två ständiga arbetsgrupper för att tillhandahålla en plattform för samarbete och utbyte mellan marknadskontrollmyndigheter och anmälande myndigheter i frågor som rör marknadskontroll respektive anmälda organ. Den ständiga arbetsgruppen för marknadskontroll bör fungera som grupp för administrativt samarbete (Adco-grupp) för denna förordning i den mening som avses i artikel 30 i förordning (EU) 2019/1020. I enlighet med artikel 33 i den förordningen bör kommissionen stödja verksamheten i den ständiga arbetsgruppen för marknadskontroll genom att genomföra marknadsutvärderingar eller marknadsstudier, särskilt i syfte att identifiera aspekter av denna förordning som kräver särskild och brådskande samordning mellan marknadskontrollmyndigheterna. Nämnden får inrätta andra ständiga eller tillfälliga undergrupper när så är lämpligt i syfte att granska specifika frågor. Nämnden bör också, när så är lämpligt, samarbeta med relevanta unionsorgan, unionsexpertgrupper och unionsnätverk som är verksamma inom ramen för relevant unionslagstiftning, särskilt de som är verksamma inom ramen för relevant unionsrätt om data, digitala produkter och tjänster.***

(150) För att säkerställa berörda parters deltagande i genomförandet och tillämpningen av denna förordning bör ett rådgivande forum inrättas för att ge råd till och tillhandahålla teknisk expertis till nämnden och kommissionen. För att säkerställa en varierad och balanserad representation av berörda parter i fråga om kommersiella och icke-kommersiella intressen samt, inom kategorin kommersiella intressen, med avseende på små och medelstora företag och andra företag, bör det rådgivande forumet bland annat omfatta industrin, nystartade företag, små och medelstora företag, den akademiska världen, det civila samhället, inbegripet arbetsmarknadens parter, samt Europeiska unionens byrå för grundläggande rättigheter, Enisa, Europeiska standardiseringskommittén (CEN), Europeiska kommittén för elektroteknisk standardisering (Cenelec) och Europeiska institutet för telekommunikationsstandarder (Etsi).

(151) För att stödja genomförandet och efterlevnaden av denna förordning, särskilt AI-byråns övervakningsverksamhet avseende AI-modeller för allmänna ändamål, bör en vetenskaplig panel av oberoende experter inrättas. De oberoende experter som ingår i den vetenskapliga panelen bör väljas ut på grundval av aktuell vetenskaplig eller teknisk expertis på AI-området och bör utföra sina uppgifter opartiskt och objektivt samt säkerställa att den information och de uppgifter som de erhåller vid utförandet av sina uppgifter och sin verksamhet behandlas konfidentiellt. För att göra det möjligt att stärka den nationella kapacitet som krävs för en effektiv efterlevnad av denna förordning bör medlemsstaterna kunna begära stöd för sin tillsynsverksamhet från poolen av experter i den vetenskapliga panelen.

(152) För att stödja en lämplig kontroll av efterlevnaden i fråga om AI-system och för att stärka medlemsstaternas kapacitet bör unionsstödstrukturer för provning av AI inrättas och göras tillgängliga för medlemsstaterna.

(153) Medlemsstaterna har en central roll i tillämpningen och kontrollen av efterlevnaden av denna förordning. I detta hänseende bör varje medlemsstat ***till*** nationella behöriga myndigheter utse ***minst en anmälande myndighet och minst en marknadskontrollmyndighet*** för att övervaka tillämpningen och genomförandet av denna förordning. ***Medlemsstaterna kan besluta att utse valfri typ av offentlig enhet för att utföra de nationella behöriga myndigheternas uppgifter i den mening som avses i denna förordning, i enlighet med sina specifika nationella organisatoriska särdrag och behov.*** För att öka den organisatoriska effektiviteten från medlemsstaternas sida och inrätta ***en gemensam*** kontaktpunkt för kontakterna med allmänheten och andra motparter på medlemsstatsnivå och unionsnivå ***bör*** ▌ varje medlemsstat ***utse en marknadskontrollmyndighet som ska fungera som gemensam kontaktpunkt***.

(154) De nationella behöriga myndigheterna bör utöva sina befogenheter på ett oberoende, objektivt och opartiskt sätt för att säkerställa principen om objektivitet i sin verksamhet och sina uppgifter och för att säkerställa tillämpningen och genomförandet av denna förordning. Ledamöterna i dessa myndigheter bör avhålla sig från varje handling som är oförenlig med deras uppdrag och bör omfattas av bestämmelserna om konfidentialitet enligt denna förordning.

(155) För att säkerställa att leverantörer av AI-system med hög risk kan beakta erfarenheterna från användning av AI-system med hög risk för att förbättra sina system och utformnings- och utvecklingsprocessen, eller kan vidta eventuella korrigerande åtgärder i rätt tid, bör alla leverantörer ha infört ett system för övervakning efter utsläppande på marknaden. ***I förekommande fall bör övervakningen efter utsläppande på marknaden omfatta en analys av interaktionen med andra AI-system, inbegripet andra enheter och programvara. Övervakningen efter utsläppande på marknaden bör inte omfatta känsliga operativa uppgifter om spridare som är brottsbekämpande myndigheter.*** Detta system är också viktigt för att säkerställa att eventuella risker som härrör från AI-system som fortsätter sin ”inlärning” efter att de släppts ut på marknaden eller tagits i bruk kan hanteras på ett mer effektivt sätt och i rätt tid. I detta sammanhang bör leverantörerna också åläggas att ha ett system för rapportering till de berörda myndigheterna av alla allvarliga incidenter ***som orsakas av användningen av deras AI-system, varmed avses en incident eller en funktionsstörning som leder till dödsfall eller allvarlig skada för hälsan, en allvarlig och oåterkallelig störning av förvaltningen och driften av kritisk infrastruktur, överträdelser av skyldigheter enligt*** unionsrätten ***avsedda att skydda*** de grundläggande rättigheterna ***eller allvarlig skada för egendom eller för miljön***.

(156) För att säkerställa ändamålsenlig och effektiv kontroll av att de krav och skyldigheter som fastställs i denna förordning och som utgör en del av unionens harmoniseringslagstiftning efterlevs bör det system för marknadskontroll och överensstämmelse för produkter som inrättas genom förordning (EU) 2019/1020 gälla i sin helhet.
Marknadskontrollmyndigheter som utsetts i enlighet med denna förordning bör ha alla de befogenheter som fastställs i denna förordning och i förordning (EU) 2019/1020 vad gäller kontroll av efterlevnad och bör utöva sina ***befogenheter och utföra sina uppgifter oberoende, objektivt och opartiskt***. ***Även om majoriteten av AI-systemen inte omfattas av särskilda krav och skyldigheter enligt denna förordning kan marknadskontroll***myndigheterna ***vidta åtgärder med avseende på alla AI-system när de utgör en risk i enlighet med denna förordning. På grund av den särskilda karaktären hos unionens institutioner, byråer och*** organ ***som omfattas av denna förordning bör Europeiska datatillsynsmannen utses till behörig marknadskontrollmyndighet för dem. Detta bör inte påverka medlemsstaternas utseende av nationella behöriga myndigheter. Marknadskontrollen*** bör ***inte påverka förmågan hos de enheter som står under tillsyn att utföra sina uppgifter på ett oberoende sätt, när ett sådant oberoende krävs enligt unionsrätten***.

(157) Denna förordning påverkar inte behörigheten, uppgifterna, befogenheterna och oberoendet för relevanta nationella offentliga myndigheter eller organ som övervakar tillämpningen av unionsrätten till skydd för de grundläggande rättigheterna, inbegripet jämställdhetsorgan och dataskyddsmyndigheter. När det är nödvändigt för dessa nationella offentliga myndigheters eller organs uppdrag bör de också ha tillgång till all dokumentation som skapas enligt denna förordning. Ett särskilt förfarande för skyddsåtgärder bör fastställas för att säkerställa adekvat och snabb kontroll av efterlevnaden gentemot AI-system som utgör en risk för hälsa, säkerhet och grundläggande rättigheter. Förfarandet för sådana AI-system som utgör en risk bör tillämpas på AI-system med hög risk som utgör en risk, på förbjudna system som har släppts ut på marknaden, tagits i bruk eller använts i strid med de bestämmelser om förbjudna metoder som fastställs i denna förordning och på AI-system som har gjorts tillgängliga i strid med de transparenskrav som fastställs i denna förordning och som utgör en risk.

(158) Unionsrätten om finansiella tjänster omfattar regler och krav för interna styrelseformer och riskhantering som är tillämpliga på reglerade finansinstitut i samband med tillhandahållandet av dessa tjänster, även när de använder AI-system. För att säkerställa en enhetlig tillämpning och kontroll av efterlevnaden av skyldigheterna enligt denna förordning och relevanta regler och krav i unionsrättsakter om finansiella tjänster, bör de ***myndigheter som är behöriga*** för tillsynen och kontrollen av efterlevnaden av dessa rättsakter, i synnerhet ***behöriga myndigheter enligt definitionen i Europaparlamentets och rådets förordning (EU) nr 575/2013[49] och*** Europa***parlamentets och rådets direktiv 2008/48/EG[50], 2009/138/EG[51], 2013/36/EU[52], 2014/17/EU[53] och (EU) 2016/97[54], inom ramen för sina respektive befogenheter,*** utses till behöriga myndigheter för tillsynen över genomförandet av denna förordning, även med avseende på marknadskontroll, när det gäller AI-system som tillhandahålls eller används av reglerade och övervakade finansinstitut, ***såvida inte medlemsstaterna beslutar att utse en annan myndighet att utföra dessa marknadskontrolluppgifter.***

---

49 Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och om ändring av förordning (EU) nr 648/2012 (EUT L 176, 27.6.2013, s. 1).

50 Europaparlamentets och rådets direktiv 2008/48/EG av den 23 april 2008 om konsumentkreditavtal och om upphävande av rådets direktiv 87/102/EEG (EUT L 133, 22.5.2008, s. 66).

51 Europaparlamentets och rådets direktiv 2009/138/EG av den 25 november 2009 om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II) (EUT L 335, 17.12.2009, s. 1).

52 Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG (EUT L 176, 27.6.2013, s. 338).

53 Europaparlamentets och rådets direktiv 2014/17/EU av den 4 februari 2014 om konsumentkreditavtal som avser bostadsfastighet och om ändring av direktiven 2008/48/EG och 2013/36/EU och förordning (EU) nr 1093/2010 (EUT L 60, 28.2.2014, s. 34).

54 Europaparlamentets och rådets direktiv (EU) 2016/97 av den 20 januari 2016 om försäkringsdistribution (EUT L 26, 2.2.2016, s. 19).

Dessa behöriga myndigheter bör ha alla befogenheter enligt denna förordning och förordning (EU) 2019/1020 för att genomdriva kraven och skyldigheterna i den här förordningen, inbegripet befogenheter att utföra efterhandskontroll av marknaden som, när så är lämpligt, kan integreras i deras befintliga tillsynsmekanismer och tillsynsförfaranden enligt relevant unionsrätt om finansiella tjänster. Det är lämpligt att de nationella myndigheter som ansvarar för tillsynen av kreditinstitut som regleras av direktiv 2013/36/EU och som deltar i den gemensamma tillsynsmekanism som inrättats genom rådets förordning (EU) nr 1024/2013[55], när de agerar som marknadskontrollmyndigheter enligt denna förordning, utan dröjsmål till Europeiska centralbanken rapporterar all information som identifierats i samband med deras marknadskontroll och som kan vara av potentiellt intresse för Europeiska centralbankens tillsynsuppgifter enligt den förordningen.

[55] Rådets förordning (EU) nr 1024/2013 av den 15 oktober 2013 om tilldelning av särskilda uppgifter till Europeiska centralbanken i fråga om politiken för tillsyn över kreditinstitut (EUT L 287, 29.10.2013, s. 63).

För att ytterligare öka konsekvensen mellan denna förordning och de regler som är tillämpliga på kreditinstitut som regleras genom direktiv 2013/36/EU är det också lämpligt att i de befintliga skyldigheterna och förfarandena enligt direktiv 2013/36/EU integrera ▌ några av leverantörernas förfarandemässiga skyldigheter vad gäller riskhantering, övervakning av produkter som släppts ut på marknaden och dokumentation. För att undvika överlappningar bör begränsade undantag också förutses när det gäller leverantörernas kvalitetsstyrningssystem och de övervakningsskyldigheter som gäller för ***spridare*** av AI-system med hög risk i den utsträckning som dessa är tillämpliga på kreditinstitut som regleras genom direktiv 2013/36/EU. ***Samma ordning bör tillämpas på försäkrings- och återförsäkringsföretag och försäkringsholdingbolag enligt direktiv 2009/138/EG och försäkringsförmedlare enligt direktiv (EU) 2016/97 och andra typer av finansinstitut som omfattas av krav avseende interna styrelseformer, arrangemang eller processer som inrättats i enlighet med relevant unionsrätt om finansiella tjänster för att säkerställa enhetlighet och likabehandling inom finanssektorn.***

(159) Varje marknadskontrollmyndighet för AI-system med hög risk på biometriområdet, enligt förteckningen i en bilaga till denna förordning, bör, i den mån dessa system används för brottsbekämpning, migration, asyl och gränskontrollförvaltning eller för rättskipning och demokratiska processer, ha effektiva utredningsbefogenheter och korrigerande befogenheter, inbegripet åtminstone befogenhet att få tillgång till alla personuppgifter som behandlas och till all information som krävs för att den ska kunna utföra sina uppgifter. Marknadskontrollmyndigheterna bör vara fullständigt oberoende i utövandet av sina befogenheter. Eventuella begränsningar av deras tillgång till känsliga operativa uppgifter enligt denna förordning bör inte påverka de befogenheter som de tilldelas genom direktiv (EU) 2016/680. Inget undantag när det gäller utlämnande av uppgifter till nationella dataskyddsmyndigheter enligt denna förordning bör påverka dessa myndigheters nuvarande eller framtida befogenheter utanför denna förordnings tillämpningsområde.

(160) Medlemsstaternas marknadskontrollmyndigheter och kommissionen bör kunna föreslå gemensamma aktiviteter, inbegripet gemensamma utredningar, som ska genomföras av marknadskontrollmyndigheterna själva eller av marknadskontrollmyndigheter tillsammans med kommissionen, och som syftar till att främja överensstämmelse, identifiera bristande överensstämmelse, öka medvetenheten och ge vägledning om denna förordning med avseende på specifika kategorier av AI-system med hög risk som befinns utgöra en allvarlig risk i två eller flera medlemsstater. Gemensamma aktiviteter för att främja överensstämmelse bör genomföras i enlighet med artikel 9 i förordning (EU) 2019/1020. AI-byrån bör tillhandahålla samordningsstöd för gemensamma utredningar.

(161) Det är nödvändigt att klargöra ansvarsområdena och befogenheterna på unionsnivå och nationell nivå när det gäller AI-system som bygger på AI-modeller för allmänna ändamål. När ett AI-system bygger på en AI-modell för allmänna ändamål och modellen och systemet tillhandahålls av samma leverantör, bör, i syfte att undvika överlappande befogenheter, tillsynen ske på unionsnivå genom AI-byrån, som bör ha befogenheter som marknadskontrollmyndighet i den mening som avses i förordning (EU) 2019/1020 för detta ändamål. I alla andra fall förblir de nationella marknadskontrollmyndigheterna ansvariga för tillsynen av AI-system. När det gäller AI-system för allmänna ändamål som kan användas direkt av spridare för minst ett ändamål som klassificeras som utgörande en hög risk bör marknadskontrollmyndigheterna dock samarbeta med AI-byrån för att utföra bedömningar av överensstämmelse och informera nämnden och andra marknadskontrollmyndigheter om detta. Dessutom bör marknadskontrollmyndigheterna kunna begära bistånd från AI-byrån om marknadskontrollmyndigheten inte kan slutföra en utredning avseende ett AI-system med hög risk på grund av att den inte får tillgång till viss information om den AI-modell för allmänna ändamål som AI-systemet med hög risk bygger på. I sådana fall bör förfarandet för ömsesidig assistans i gränsöverskridande fall i kapitel VI i förordning (EU) 2019/1020 gälla i tillämpliga delar.

(162) I syfte att på bästa sätt utnyttja unionens centraliserade sakkunskap och synergier på unionsnivå bör befogenheterna avseende tillsyn och kontroll av efterlevnaden av skyldigheterna för leverantörer av AI-modeller för allmänna ändamål omfattas av kommissionens behörighet. Kommissionen bör anförtro genomförandet av dessa uppgifter till AI-byrån, utan att det påverkar kommissionens organisationsbefogenheter och befogenhetsfördelningen mellan medlemsstaterna och unionen på grundval av fördragen. AI-byrån bör kunna vidta alla nödvändiga åtgärder för att övervaka det effektiva genomförandet av denna förordning när det gäller AI-modeller för allmänna ändamål. Den bör kunna utreda eventuella överträdelser av reglerna för leverantörer av AI-modeller för allmänna ändamål, både på eget initiativ, baserat på resultaten av dess övervakningsverksamhet, eller på begäran av marknadskontrollmyndigheterna i enlighet med villkoren i denna förordning. I syfte att stödja en effektiv övervakning genom AI-byrån bör det föreskrivas en möjlighet för leverantörer i efterföljande led att lämna in klagomål om eventuella överträdelser av reglerna för leverantörer av AI-system för allmänna ändamål.

(163) I syfte att komplettera styrningssystemen för AI-modeller för allmänna ändamål bör den vetenskapliga panelen stödja AI-byråns övervakningsverksamhet och får, i vissa fall, tillhandahålla kvalificerade varningar till AI-byrån som utlöser uppföljningar, såsom utredningar. Detta bör vara fallet om den vetenskapliga panelen har skäl att misstänka att en AI-modell för allmänna ändamål utgör en konkret och identifierbar risk på unionsnivå. Detta bör dessutom vara fallet om den vetenskapliga panelen har skäl att misstänka att en AI-modell för allmänna ändamål uppfyller kriterierna för att klassificeras som en AI-modell för allmänna ändamål med systemrisk. I syfte att förse den vetenskapliga panelen med den information som krävs för utförandet av dessa uppgifter bör det finnas en mekanism genom vilken den vetenskapliga panelen kan uppmana kommissionen att begära dokumentation eller information från en leverantör.

(164) AI-byrån bör kunna vidta nödvändiga åtgärder för att övervaka det faktiska genomförandet och efterlevnaden av de skyldigheter för leverantörer av AI-modeller för allmänna ändamål som fastställs i denna förordning. AI-byrån bör kunna utreda eventuella överträdelser i enlighet med de befogenheter som föreskrivs i denna förordning, bland annat genom att begära dokumentation och information, genom att genomföra utvärderingar och genom att kräva åtgärder från leverantörer av AI-modeller för allmänna ändamål. Vid genomförandet av utvärderingar bör AI-byrån, i syfte att utnyttja oberoende sakkunskap, kunna anlita oberoende experter som kan utföra utvärderingarna för dess räkning. Efterlevnaden av skyldigheterna bör kunna verkställas, bland annat genom begäranden om att vidta lämpliga åtgärder, inbegripet riskbegränsningsåtgärder i händelse av identifierade systemrisker samt begränsning av tillhandahållandet på marknaden, tillbakadragande eller återkallande av modellen. Som en skyddsåtgärd, när detta behövs utöver de processuella rättigheter som föreskrivs i denna förordning, bör leverantörer av AI-modeller för allmänna ändamål ha de processuella rättigheter som föreskrivs i artikel 18 i förordning (EU) 2019/1020, som bör gälla i tillämpliga delar, utan att det påverkar de mer specifika processuella rättigheter som föreskrivs i den här förordningen.

(165) Utvecklingen av andra AI-system än AI-system med hög risk i enlighet med kraven i denna förordning kan leda till en ökad användning av ***etisk och*** tillförlitlig AI i unionen. Leverantörer av AI-system som inte utgör hög risk bör uppmuntras att ta fram uppförandekoder***, inbegripet tillhörande styrningsmekanismer,*** avsedda att främja en frivillig tillämpning av ***vissa eller alla av*** de obligatoriska krav som gäller för AI-system med hög risk***, anpassade med hänsyn till systemens avsedda ändamål och den lägre risk som de medför och med beaktande av tillgängliga tekniska lösningar och bästa branschpraxis, såsom modellkort och datakort***. Leverantörerna ***och, i förekommande fall, spridarna av alla AI-system, med eller utan hög risk, och AI-modeller*** bör också uppmuntras att på frivillig grund tillämpa ytterligare krav avseende exempelvis ***inslagen i unionens etiska riktlinjer för tillförlitlig AI,*** miljömässig hållbarhet, ***åtgärder för AI-kunskap, inkluderande och diversifierad utformning och utveckling av AI-system, inbegripet uppmärksamhet för sårbara personer och*** tillgänglighet för personer med funktionsnedsättning, berörda parters deltagande ***med medverkan, i förekommande fall, av sådana berörda parter som näringslivsorganisationer och det civila samhällets organisationer, den akademiska världen, forskningsorganisationer, fackföreningar och konsumentskyddsorganisationer*** i utformningen och utvecklingen av AI-system samt mångfald i utvecklingsteamen***, inbegripet en jämn könsfördelning. För att säkerställa att de frivilliga uppförandekoderna är effektiva bör de grunda sig på tydliga mål och nyckelprestationsindikatorer för att mäta uppnåendet av dessa mål. De bör också utvecklas på ett inkluderande sätt, när så är lämpligt, med deltagande av berörda parter såsom näringslivsorganisationer och det civila samhällets organisationer, den akademiska världen, forskningsorganisationer, fackföreningar och konsumentskyddsorganisationer***. Kommissionen kan utveckla initiativ, även på sektorsbasis, för att minska de tekniska hindren för gränsöverskridande utbyte av data för AI-utveckling, däribland vad gäller infrastruktur för dataåtkomst samt semantisk och teknisk interoperabilitet för olika typer av data.

(166) Det är viktigt att AI-system som avser produkter som inte utgör hög risk enligt denna förordning och som därmed inte måste uppfylla kraven ***på AI-system med hög risk*** ändå är säkra när de släpps ut på marknaden eller tas i bruk. För att bidra till detta mål skulle Europaparlamentets och rådets ***förordning (EU) 2023/988***[56] tillämpas som ett skyddsnät.

(167) För att säkerställa ett förtroendefullt och konstruktivt samarbete mellan behöriga myndigheter på unionsnivå och nationell nivå bör alla parter som är involverade i tillämpningen av denna förordning säkerställa konfidentiell behandling av information och data som de erhåller i utförandet av sina uppgifter, ***i enlighet med unionsrätten eller nationell rätt***. ***De bör utföra sina uppgifter och sin verksamhet på ett sådant sätt att de i synnerhet skyddar immateriella rättigheter, konfidentiell affärsinformation och företagshemligheter, det effektiva genomförandet av denna förordning, allmänna och nationella säkerhetsintressen, integriteten i straffrättsliga och administrativa förfaranden samt integriteten hos säkerhetsskyddsklassificerade uppgifter.***

[56] Europaparlamentets och rådets ***förordning (EU) 2023/988*** av den ***10 maj 2023*** om allmän produktsäkerhet***, ändring av Europaparlamentets och rådets förordning (EU) nr 1025/2012 och Europaparlamentets och rådets direktiv (EU) 2020/1828 och om upphävande av Europaparlamentets och rådets direktiv 2001/95/EG och rådets direktiv 87/357/EEG (EUT L 135, 23.5.2023, s. 1)***.

(168) ***Efterlevnaden av denna förordning bör kunna verkställas genom ålläggande av sanktioner och andra verkställighetsåtgärder.*** Medlemsstaterna bör vidta alla nödvändiga åtgärder för att säkerställa att bestämmelserna i denna förordning genomförs, bland annat genom att fastställa effektiva, proportionella och avskräckande sanktioner för åsidosättande av dem***, inbegripet med iakttagande av principen ne bis in idem. För att stärka och harmonisera de administrativa sanktionerna för överträdelser av denna förordning bör det fastställas övre gränser för fastställande av administrativa sanktionsavgifter*** för vissa specifika överträdelser. ***Vid bedömningen av storleken på sanktionsavgifterna*** bör medlemsstaterna ***i varje enskilt fall*** beakta ***alla relevanta omständigheter i den specifika situationen, med vederbörlig hänsyn särskilt till överträdelsens art, svårighetsgrad och varaktighet och dess konsekvenser samt till leverantörens storlek, särskilt ifall leverantören tillhör kategorin små och medelstora företag, inbegripet nystartade företag***. Europeiska datatillsynsmannen bör ha befogenhet att ålägga böter för unionens institutioner, byråer och organ som omfattas av denna förordning.

(169) Efterlevnaden av de skyldigheter för leverantörer av AI-modeller för allmänna ändamål som införs enligt denna förordning bör kunna verkställas bland annat genom sanktionsavgifter. I detta syfte bör lämpliga nivåer på sanktionsavgifterna också fastställas för överträdelser av dessa skyldigheter, inbegripet åsidosättande av de åtgärder som kommissionen begär i enlighet med denna förordning, med förbehåll för lämpliga preskriptionstider i enlighet med proportionalitetsprincipen. Alla beslut som kommissionen fattar enligt denna förordning kan prövas av Europeiska unionens domstol i enlighet med EUF-fördraget.

(170) Unionsrätten och nationell rätt föreskriver redan effektiva rättsmedel för fysiska och juridiska personer vars rättigheter och friheter påverkas negativt av användningen av AI-system. Utan att det påverkar dessa rättsmedel bör varje fysisk eller juridisk person som har skäl att anse att denna förordning har överträtts ha rätt att lämna in klagomål till den berörda marknadskontrollmyndigheten.

(171) Berörda personer bör ha rätt att få en förklaring om en spridares beslut huvudsakligen grundar sig på utdata från vissa högrisksystem som omfattas av denna förordning och om det beslutet har rättslig verkan eller på liknande sätt i betydande grad påverkar dessa personer på ett sätt som de anser ha en negativ inverkan på deras hälsa, säkerhet eller grundläggande rättigheter. Den förklaringen bör vara tydlig och meningsfull och bör tillhandahålla en grund på vilken de berörda personerna kan utöva sina rättigheter. Rätten att få en förklaring bör inte tillämpas på sådan användning av AI-system som enligt unionsrätten eller nationell rätt omfattas av undantag eller begränsningar och bör endast tillämpas i den mån denna rätt inte redan föreskrivs i unionsrätten.

(172) Personer som agerar som visselblåsare när det gäller överträdelser av denna förordning bör skyddas enligt unionsrätten. Europaparlamentets och rådets direktiv (EU) 2019/1937[57] bör därför tillämpas på rapportering av överträdelser av denna förordning och skydd för personer som rapporterar om sådana överträdelser.

[57] Europaparlamentets och rådets direktiv (EU) 2019/1937 av den 23 oktober 2019 om skydd för personer som rapporterar om överträdelser av unionsrätten (EUT L 305, 26.11.2019, s. 17).

(173) För att säkerställa att regelverket vid behov kan anpassas bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen när det gäller ändring av de villkor enligt vilka ett AI-system inte ska betraktas som högrisksystem, förteckningen över AI-system med hög risk, bestämmelserna om teknisk dokumentation, innehållet i EU-försäkran om överensstämmelse, bestämmelserna om förfaranden för bedömning av överensstämmelse***,*** bestämmelserna om fastställande av de AI-system med hög risk som omfattas av det förfarande för bedömning av överensstämmelse som baseras på en bedömning av kvalitetsstyrningssystemet och en bedömning av den tekniska dokumentationen***, tröskelvärdet, riktmärkena och indikatorerna, bland annat genom komplettering av dessa riktmärken och indikatorer, i reglerna för klassificering av AI-modeller för allmänna ändamål med systemrisk, kriterierna för utseende av AI-modeller för allmänna ändamål med systemrisk, den tekniska dokumentationen för leverantörer av AI-modeller för allmänna ändamål och transparensinformationen för leverantörer av AI-modeller för allmänna ändamål***. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning[58]. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

[58] EUT L 123, 12.5.2016, s. 1.

(174) Med tanke på den snabba tekniska utvecklingen och den tekniska expertis som krävs för en effektiv tillämpning av denna förordning bör kommissionen utvärdera och se över denna förordning senast den ... [fem år efter dagen för denna förordnings ikraftträdande] och därefter vart fjärde år samt rapportera till Europaparlamentet och rådet. Dessutom bör kommissionen, med beaktande av konsekvenserna för denna förordnings tillämpningsområde, en gång om året göra en bedömning av behovet av att ändra förteckningen över AI-system med hög risk och förteckningen över förbjudna metoder. Senast två år efter tillämpningsdagen och därefter vart fjärde år bör kommissionen dessutom utvärdera och till Europaparlamentet och rådet rapportera om behovet av att ändra förteckningen över högriskområden i bilagan till denna förordning, de AI-system som omfattas av transparensskyldigheterna, tillsyns- och styrningssystemets effektivitet och framstegen med utvecklingen av standardiseringsprodukter för energieffektiv utveckling av AI-modeller för allmänna ändamål, inbegripet behovet av ytterligare åtgärder eller insatser. Senast den ... [fyra år efter denna förordnings ikraftträdande] och därefter vart tredje år bör kommissionen slutligen utvärdera inverkan och effektiviteten hos de frivilliga uppförandekoder som syftar till att främja tillämpningen av de krav som fastställs för AI-system med hög risk när det gäller andra AI-system än AI-system med hög risk och eventuellt andra ytterligare krav för sådana AI-system.

(175) För att säkerställa enhetliga villkor för genomförandet av denna förordning, bör kommissionen tilldelas genomförandebefogenheter. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011[59].

(176) Eftersom målet för denna förordning, nämligen att förbättra den inre marknadens funktion och främja användningen av människocentrerad och tillförlitlig AI, samtidigt som en hög skyddsnivå säkerställs för hälsa, säkerhet och grundläggande rättigheter som fastställs i stadgan, inbegripet demokrati, rättsstatsprincipen och miljöskydd, mot de skadliga effekterna av AI-system i unionen, och att stödja innovation, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i EU-fördraget. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

[59] Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

(177) För att säkerställa rättslig säkerhet, säkerställa en lämplig anpassningsperiod för operatörer och undvika störningar på marknaden, bland annat genom att säkerställa kontinuitet i användningen av AI-system, bör denna förordning tillämpas på AI-system med hög risk som har släppts ut på marknaden eller tagits i bruk före den allmänna tillämpningsdagen för förordningen, endast om dessa system från och med den dagen genomgår betydande ändringar av sin utformning eller sitt avsedda ändamål. Det är lämpligt att klargöra att begreppet betydande ändring i detta avseende bör tolkas som att det i sak är likvärdigt med begreppet väsentlig ändring, som endast används med avseende på AI-system med hög risk i enlighet med denna förordning. I undantagsfall och mot bakgrund av offentlig ansvarsskyldighet bör operatörer av AI-system som är komponenter i de stora it-system som inrättats genom de rättsakter som förtecknas i en bilaga till denna förordning respektive operatörer av AI-system med hög risk som är avsedda att användas av offentliga myndigheter vidta nödvändiga åtgärder för att uppfylla kraven i denna förordning senast i slutet av 2030 och senast sex år efter ikraftträdandet.

(178) Leverantörer av AI-system med hög risk uppmuntras att på frivillig basis börja fullgöra de relevanta skyldigheterna i denna förordning redan under övergångsperioden.

(179) Denna förordning bör tillämpas från och med den ... [två år efter dagen för denna förordnings ikraftträdande]. ***Med hänsyn till den oacceptabla risk som är förknippad med användning av AI på vissa sätt bör*** dock ***förbuden tillämpas redan från och med den... [sex månader från och med den dag då denna förordning träder i kraft]. Även om dessa förbuds fulla verkan följer av inrättandet av styrningen och verkställigheten av denna förordning, är det viktigt att föregripa tillämpningen av förbuden för att ta hänsyn till oacceptabla risker och påverka andra förfaranden, t.ex. civilrättsliga förfaranden. Vidare*** bör infrastrukturen för styrning och systemet för bedömning av överensstämmelse vara operativa före det datumet, varför bestämmelserna om anmälda organ och styrningsstruktur bör tillämpas från och med den … [***12*** månader ***från dagen för*** denna förordnings ikraftträdande]. ***Med tanke på den snabba takten inom tekniska framsteg och införandet av AI-modeller för allmänna ändamål bör skyldigheterna för leverantörer av AI-modeller för allmänna ändamål gälla från och med den … [12 månader från dagen för denna förordnings ikraftträdande]. Förfarandekoder bör vara klara senast den ...*** [***9*** **månader** ***från dagen för*** denna förordnings ***ikraftträdande] för att leverantörer ska kunna visa efterlevnad i tid. AI-byrån bör säkerställa att klassificeringsregler och klassificeringsförfaranden är aktuella mot bakgrund av den tekniska utvecklingen.*** Medlemsstaterna bör också fastställa och meddela kommissionen reglerna om sanktioner, inklusive administrativa sanktionsavgifter, och säkerställa att de genomförs korrekt och effektivt senast den dag då denna förordning börjar tillämpas. Därför bör bestämmelserna om sanktioner tillämpas från och med den … [12 månader från dagen för denna förordnings ikraftträdande].

(180) Europeiska datatillsynsmannen och Europeiska dataskyddsstyrelsen har hörts i enlighet med artikel 42.1 och 42.2 i förordning (EU) 2018/1725 och avgav sitt gemensamma yttrande den ▌ ***18 juni 2021***.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I
ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll

1. ***Syftet med denna förordning är att förbättra den inre marknadens funktion och främja användningen av människocentrerad och tillförlitlig artificiell intelligens (AI), samtidigt som en hög skyddsnivå säkerställs för hälsa, säkerhet och grundläggande rättigheter som fastställs i stadgan om de grundläggande rättigheterna, inbegripet demokrati, rättsstatsprincipen och miljöskydd, mot de skadliga effekterna av system för artificiell intelligens*** (AI-system) ***i unionen, och att stödja innovation***.

2. I denna förordning fastställs

a) harmoniserade regler för utsläppande på marknaden, ibruktagande och användning av AI-system i unionen,

b) förbud mot vissa AI-metoder,

c) särskilda krav för AI-system med hög risk och skyldigheter för operatörer av sådana system,

d) harmoniserade transparensregler för ***vissa*** AI-system***,***

e) harmoniserade regler för utsläppande på marknaden av AI-modeller för allmänna ändamål,

f) regler om marknadsövervakning***, styrning av marknadskontroll och verkställighet,***

g) åtgärder till stöd för innovation med särskild inriktning på små och medelstora företag och nystartade företag.

Artikel 2

Tillämpningsområde

1. Denna förordning ska tillämpas på

a) leverantörer som släpper ut AI-system på marknaden eller tar sådana i bruk ***eller släpper ut AI-modeller för allmänna ändamål på marknaden*** i unionen, oavsett om dessa leverantörer är etablerade ***eller befinner sig*** i unionen eller i ett tredjeland,

b) ***spridare*** av AI-system ***som har sin etableringsort eller*** befinner sig i unionen,

c) leverantörer och ***spridare*** av AI-system ***som har sin etableringsort eller*** befinner sig i ett tredjeland, om de utdata som produceras av AI-systemet används i unionen,

d) importörer och distributörer av AI-system,

e) produkttillverkare som på marknaden släpper ut eller som tar i bruk ett AI-system tillsammans med sin produkt och i eget namn eller under eget varumärke,

f) ombud för leverantörer som inte är etablerade i unionen,

g) berörda personer som befinner sig i unionen.

2. För ▌ AI-system ***som klassificeras som AI-system med hög risk enligt artikel 6.1 och 6.2 och som är relaterade till*** produkter som omfattas ***av den unionslagstiftning om harmonisering som förtecknas i avsnitt B i bilaga I*** ska endast artikel 112 tillämpas: ***Artikel 57 ska tillämpas endast i den mån som kraven för AI-system med hög risk enligt denna förordning har integrerats i denna unionslagstiftning om harmonisering.***

▌

3. ***Denna förordning ska inte tillämpas på områden som inte omfattas av tillämpningsområdet för unionsrätten och ska i vilket fall inte påverka medlemsstaternas befogenheter när det gäller nationell säkerhet, oavsett vilken typ av enhet som medlemsstaterna anförtrott uppgiften i fråga om dessa befogenheter.***

Denna förordning ska inte tillämpas på AI-system, ***om och i den mån de släpps ut på marknaden, tas i bruk eller används med eller utan ändring uteslutande för militära ändamål, försvarsändamål eller ändamål som rör nationell säkerhet, oavsett vilken typ av enhet som bedriver denna verksamhet***.

Denna förordning ska inte tillämpas på AI-system som inte släpps ut på marknaden eller tas i bruk i unionen, om utdata används i unionen uteslutande för militära ändamål***, försvarsändamål eller*** ändamål ***som rör nationell säkerhet, oavsett vilken typ av enhet som bedriver denna verksamhet***.

4. Denna förordning ska inte tillämpas på offentliga myndigheter i ett tredjeland, eller på internationella organisationer som omfattas av denna förordnings tillämpningsområde enligt punkt 1, om dessa myndigheter eller organisationer använder AI-system inom ramen för ***internationellt samarbete eller*** internationella avtal om brottsbekämpande och rättsligt samarbete med unionen eller med en eller flera medlemsstater***, förutsatt att ett sådant tredjeland eller en sådan internationell organisation erbjuder lämpliga skyddsåtgärder med avseende på skyddet av enskildas grundläggande rättigheter och friheter***.

5. Denna förordning ska inte påverka tillämpningen av bestämmelserna om ansvar för leverantörer av förmedlingstjänster i kapitel II i förordning (EU) 2022/2065.

6. Denna förordning ska inte tillämpas på AI-system eller AI-modeller, inbegripet deras utdata, som specifikt utvecklas och tas i bruk enbart i vetenskapligt forsknings- och utvecklingssyfte.

7. Unionsrätt om skydd av personuppgifter, integritet och konfidentialitet vid kommunikation är tillämplig på personuppgifter som behandlas i samband med de rättigheter och skyldigheter som fastställs i denna förordning. Denna förordning ska inte påverka tillämpningen av förordning (EU) 2016/679 eller (EU) 2018/1725 eller direktiv 2002/58/EG eller (EU) 2016/680, utan att det påverkar tillämpningen av de arrangemang som föreskrivs i artiklarna 10.5 och 59 i den här förordningen.

8. Denna förordning ska inte tillämpas på forsknings-, testnings- eller utvecklingsverksamhet för AI-system eller AI-modeller före deras utsläppande på marknaden eller ibruktagande. Sådan verksamhet ska bedrivas i enlighet med tillämplig unionsrätt. Testning under verkliga förhållanden ska inte omfattas av detta undantag.

9. Denna förordning påverkar inte tillämpningen av de regler som fastställs genom andra unionsrättsakter om konsumentskydd och produktsäkerhet.

10. Denna förordning ska inte tillämpas på skyldigheter för spridare som är fysiska personer som använder AI-system inom ramen för en rent personlig icke-yrkesmässig verksamhet.

11. Denna förordning ska inte hindra unionen eller medlemsstaterna att behålla eller införa lagar och andra författningar som är förmånligare för arbetstagarna när det gäller att skydda deras rättigheter i fråga om arbetsgivares användning av AI-system, eller att uppmuntra eller tillåta tillämpning av kollektivavtal som är förmånligare för arbetstagarna.

12. Denna förordning ska tillämpas på AI-system som släpps ut inom ramen för fria licenser med öppen källkod, såvida de inte släpps ut på marknaden eller tas i bruk som ett AI-system med hög risk eller som ett AI-system som omfattas av artikel 5 eller 50.

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

1. ***AI-****system*: ***ett maskinbaserat system som är utformat för att fungera med varierande grad av autonomi, som kan uppvisa anpassningsförmåga efter införande och som, för uttryckliga eller underförstådda mål, på grundval av de indata det tar emot, drar slutsatser om hur*** utdata såsom ***förutsägelser, innehåll,*** rekommendationer eller beslut ***som kan påverka fysiska eller virtuella*** miljöer ska genereras.

2. risk: kombinationen av sannolikheten för skada och denna skadas allvarlighetsgrad.

3. *leverantör*: en fysisk eller juridisk person, en offentlig myndighet, en byrå eller ett annat organ som utvecklar ett AI-system ***eller en AI-modell för allmänna ändamål och släpper ut det eller den*** på marknaden ***eller tar AI-systemet*** i bruk i eget namn eller under eget varumärke, antingen mot betalning eller kostnadsfritt.

4. *spridare*: en fysisk eller juridisk person, offentlig myndighet, en byrå eller annat organ som under eget överinseende ▌ använder ett AI-system, utom när AI-systemet används inom ramen för en personlig icke-yrkesmässig verksamhet.

5. *ombud*: en fysisk eller juridisk person ***som befinner sig eller*** är etablerad i unionen och som har fått ***och godtagit*** en skriftlig fullmakt från en leverantör av ett AI-system ***eller av en AI-modell för allmänna ändamål*** för att för dennes räkning fullgöra respektive genomföra de skyldigheter och förfaranden som fastställs i denna förordning.

6. *importör*: en fysisk eller juridisk person ***som befinner sig eller*** är etablerad i unionen och som släpper ut ett ▌ AI-system på marknaden som bär namnet på eller varumärket för en fysisk eller juridisk person som är etablerad i ett tredjeland.

7. *distributör*: en annan fysisk eller juridisk person i leveranskedjan som tillhandahåller ett AI-system på unionsmarknaden än leverantören eller importören ▌ .

8. *operatör*: en leverantör, ***en produkttillverkare, en spridare***, ett ombud, en importör ***eller*** en distributör.

9. *utsläppande på marknaden*: den första gången ett AI-system ***eller en AI-modell för allmänna ändamål*** tillhandahålls på unionsmarknaden.

10. *tillhandahållande på marknaden*: leveransen av ett AI-system ***eller en AI-modell för allmänna ändamål*** för distribution eller användning på unionsmarknaden i samband med kommersiell verksamhet, mot betalning eller kostnadsfritt.

11. *ibruktagande*: leverans av ett AI-system av leverantören för första användning direkt till ***spridaren*** eller för eget bruk ***i*** unionen ▌ för dess avsedda ändamål.

12. *avsett ändamål*: den användning för vilken ett AI-system är avsett av leverantören, inbegripet det specifika användningssammanhanget och de specifika användningsvillkoren, enligt specifikationerna i de uppgifter som tillhandahålls av leverantören i bruksanvisningen, reklam- eller försäljningsmaterial och uttalanden samt i den tekniska dokumentationen.

13. *rimligen förutsebar felaktig användning*: användning av ett AI-system på ett sätt som inte överensstämmer med dess avsedda ändamål, men som kan vara resultatet av rimligen förutsebart mänskligt beteende eller interaktion med andra system***, inbegripet andra AI-system***.

14. *säkerhetskomponent*: en komponent som finns i en produkt eller i ett system och som fyller en säkerhetsfunktion för produkten eller systemet eller som, om den upphör att fungera eller fungerar felaktigt, medför fara för människors hälsa och säkerhet eller för egendom.

15. *bruksanvisning*: information som tillhandahålls av leverantören för att informera spridaren om särskilt ett AI-systems avsedda ändamål och korrekta användning ▌ .

16. *återkallelse av ett AI-system:* varje åtgärd som syftar till att få till stånd ett återlämnande till leverantören***, ett urdrifttagande eller en avaktivering av användningen*** av ett AI-system som tillhandahållits för ***spridare***.

17. *tillbakadragande av ett AI-system*: varje åtgärd som syftar till att förhindra ***att ett AI-system i leveranskedjan tillhandahålls på marknaden***.

18. *ett AI-systems prestanda*: ett AI-systems förmåga att uppnå sitt avsedda ändamål.

19. *anmälande myndighet*: den nationella myndighet som ansvarar för inrättandet och genomförandet av de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och för övervakning av dessa.

20. *bedömning av överensstämmelse*: processen att ***visa*** om kraven i kapitel II avsnitt 2 avseende ***ett*** AI-system ***med hög risk*** har uppfyllts.

21. *organ för bedömning av överensstämmelse*: organ som utför tredjepartsbedömning av överensstämmelse, inbegripet testning, certifiering och inspektion.

22. *anmält organ*: organ för bedömning av överensstämmelse som ***anmälts*** i enlighet med denna förordning och annan relevant unionslagstiftning om harmonisering som förtecknas i bilaga I avsnitt B.

23. *väsentlig ändring*: en ändring av ett AI-system ***efter*** dess utsläppande på marknaden eller ibruktagande som ***inte förutsetts eller planerats i leverantörens ursprungliga bedömning av överensstämmelse och som leder till att*** AI-systemets uppfyllelse av kraven i kapitel II avdelning 2 ***påverkas*** eller leder till en ändring av det avsedda ändamål för vilket AI-systemet har bedömts.

24. *CE-märkning*: märkning genom vilken en leverantör anger att ett AI-system överensstämmer med kraven i kapitel II avsnitt 2 och annan tillämplig unionslagstiftning om harmonisering som förtecknas i bilaga I och som föreskriver att den anbringas.

25. ***system*** *för övervakning efter utsläppande på marknaden*: all verksamhet som bedrivs av leverantörer av AI-system för att ▌ samla in och granska erfarenheter från användningen av AI-system som de släpper ut på marknaden eller tar i bruk, i syfte att fastställa ett eventuellt behov av att omedelbart vidta eventuella nödvändiga korrigerande eller förebyggande åtgärder.

26. *marknadskontrollmyndighet*: den nationella myndighet som utför aktiviteter och vidtar åtgärder enligt förordning (EU) 2019/1020.

27. *harmoniserad standard*: en harmoniserad standard enligt definitionen i artikel 2.1 c i förordning (EU) nr 1025/2012.

28. *gemensam* ***specifikation***: en ***uppsättning tekniska specifikationer enligt definitionen i artikel 2.4 i förordning (EU) nr 1025/2012 som ger*** förutsättningar för att ▌ uppfylla vissa krav ▌ som fastställts enligt den här förordningen.

29. *träningsdata*: data som används för att träna ett AI-system genom anpassning av dess inlärningsbara parametrar ▌ .

30. *valideringsdata*: data som används för att tillhandahålla en utvärdering av det tränade AI-systemet och för att stämma av dess icke-inlärningsbara parametrar och dess inlärningsprocess för att bland annat förhindra ***under- eller*** över***anpassning***.

31. *valideringsdataset*: ett separat dataset eller en separat del av träningsdatasetet, antingen som en fast eller variabel uppdelning.

32. *testdata*: data som används för att tillhandahålla en oberoende utvärdering av ▌ AI-systemet för att bekräfta systemets förväntade prestanda innan det släpps ut på marknaden eller tas i bruk.

33. *indata*: data som lämnas till eller anskaffas direkt av ett AI-system och som utgör den grund på vilken systemet producerar utdata.

34. *biometriska uppgifter*: personuppgifter som erhållits genom särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken, ▌ såsom ansiktsbilder eller fingeravtrycksuppgifter.

35. biometrisk identifiering: automatiserad igenkänning av fysiska, fysiologiska, beteendemässiga eller psykologiska mänskliga särdrag för att fastställa en fysisk persons identitet genom jämförelse av personens biometriska uppgifter med biometriska uppgifter om enskilda personer som lagrats i en databas.

36. biometrisk verifiering: automatiserad en-till-en-verifiering, inklusive autentisering, av fysiska personers identitet genom jämförelse av deras biometriska uppgifter med tidigare lämnade biometriska uppgifter.

37. särskilda kategorier av personuppgifter: de kategorier av personuppgifter som avses i artikel 9.1 i förordning (EU) 2016/679, artikel 10 i direktiv (EU) 2016/680 och artikel 10.1 i förordning (EU) 2018/1725.

38. känsliga operativa uppgifter: operativa uppgifter som rör verksamhet för att förebygga, förhindra, utreda, avslöja eller lagföra brott och vars röjande skulle kunna äventyra straffrättsliga förfarandens integritet.

39. *system för känsloigenkänning*: ett AI-system vars syfte är att identifiera eller uttyda fysiska personers känslor eller avsikter på grundval av deras biometriska uppgifter.

40. *system för biometrisk kategorisering*: ett AI-system för hänförande av fysiska personer till särskilda kategorier ***på grundval av deras biometriska uppgifter, om det inte utgör en extrafunktion till en annan kommersiell tjänst och är strikt nödvändigt av objektiva tekniska skäl.***

41. *system för biometrisk fjärridentifiering*: ett AI-system vars syfte är att identifiera fysiska personer ***utan deras aktiva medverkan, vanligtvis*** på distans, genom jämförelse av en persons biometriska uppgifter med de biometriska uppgifterna i en referensdatabas ▌ .

42. *system för biometrisk fjärridentifiering i realtid*: ett system för biometrisk fjärridentifiering där infångning av biometriska uppgifter, jämförelse och identifiering sker utan betydande dröjsmål och omfattar inte bara omedelbar identifiering utan även begränsade korta fördröjningar för att undvika kringgående.

43. *system för biometrisk fjärridentifiering i efterhand*: ett annat system för biometrisk fjärridentifiering än ett system för biometrisk fjärridentifiering i realtid.

44. *allmänt tillgänglig plats*: varje ***offentlig- eller privatägd*** fysisk plats som är tillgänglig för ***ett obestämt antal fysiska personer***, utan hänsyn till om vissa villkor eller omständigheter för tillträde kan gälla***, och oberoende av eventuella kapacitetsbegränsningar***.

45. *brottsbekämpande myndighet*:

a) en offentlig myndighet som har behörighet att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inbegripet att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, eller

b) ett annat organ eller en annan enhet som genom medlemsstaternas nationella rätt har anförtrotts myndighetsutövning för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inbegripet att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

46. *brottsbekämpning*: verksamhet som genomförs av brottsbekämpande myndigheter ***eller på deras vägnar*** för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inbegripet att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

47. ***AI-byrån: kommissionens funktion att bidra till genomförandet, övervakningen och tillsynen av AI-system och AI-styrning, som utförs av Europeiska byrån för artificiell intelligens, som inrättades genom kommissionens beslut av den 24 januari 2024; hänvisningar i denna förordning till AI-byrån ska anses som hänvisningar till kommissionen.***

48. *nationell behörig myndighet*: ***en*** anmälande myndighet eller en marknadskontrollmyndighet.

49. *allvarlig incident*: en incident ***eller ett fel i ett AI-system som direkt eller indirekt orsakar*** något av följande:

a) Dödsfall eller allvarlig skada på en persons hälsa.

b) En allvarlig och oåterkallelig störning av förvaltningen eller driften av kritisk infrastruktur.

c) Åsidosättande ***av skyldigheter enligt unionsrätten avsedda att skydda grundläggande rättigheter.***

d) Allvarlig skada på egendom eller på miljön.

50. personuppgifter: personuppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.

51. icke-personuppgifter: andra uppgifter än personuppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.

52. profilering: profilering enligt definitionen i artikel 4.4 i förordning (EU) 2016/679, eller, när det gäller brottsbekämpande myndigheter, enligt definitionen i artikel 3.4 i direktiv (EU) 2016/680, eller, när det gäller unionens institutioner, organ eller byråer, enligt definitionen i artikel 3.5 i förordning (EU) 2018/1725.

53. plan för testning under verkliga förhållanden: ett dokument som beskriver målen och metoden för samt den geografiska, befolkningsmässiga och tidsmässiga omfattningen, övervakningen, organisationen samt genomförandet av testning under verkliga förhållanden.

54. sandlådeplan: ett dokument om vilket den deltagande leverantören och den behöriga myndigheten har kommit överens och som beskriver målen, villkoren, tidsplanen, metoden och kraven för den verksamhet som ska bedrivas i sandlådan.

55. regulatorisk sandlåda för AI: en kontrollerad ram som inrättats av en behörig myndighet och som erbjuder leverantörer eller potentiella leverantörer av AI-system möjlighet att utveckla, träna, validera och testa, när så är lämpligt under verkliga förhållanden, ett innovativt AI-system, i enlighet med en specifik sandlådeplan för en begränsad tid under regulatorisk tillsyn.

56. AI-kunskap: kompetens, kunskap och förståelse som gör det möjligt för leverantörer, spridare och berörda personer att, med hänsyn till deras respektive rättigheter och skyldigheter i samband med denna förordning, införa AI-system på ett välgrundat sätt samt bli medvetna om möjligheterna och riskerna med AI, och den potentiella skada den kan vålla.

57. testning under verkliga förhållanden: tillfällig testning av ett AI-system med avseende på dess avsedda ändamål under verkliga förhållanden utanför ett laboratorium eller en på annat sätt simulerad miljö i syfte att samla in tillförlitliga och robusta data och bedöma och kontrollera AI-systemets överensstämmelse med kraven i denna förordning, och den ska inte anses innebära att AI-systemet släpps ut på marknaden eller tas i bruk i den mening som avses i denna förordning, förutsatt att alla villkor enligt artikel 57 eller 60 är uppfyllda;

58. försöksperson: vid testning under verkliga förhållanden en fysisk person som deltar i testning under verkliga förhållanden.

59. informerat samtycke: en försökspersons frivilliga, specifika, informerade och otvetydiga uttryck för sin vilja att delta i en viss testning under verkliga förhållanden, efter att ha informerats om alla aspekter av testningen som är relevanta för försökspersonens beslut att delta.

60. deepfake: AI-genererat eller AI-manipulerat bild-, ljud- eller videoinnehåll som liknar existerande personer, föremål, platser eller andra enheter eller händelser och som felaktigt skulle kunna uppfattas som autentiskt eller sanningsenligt.

61. utbredd överträdelse: varje handling eller underlåtenhet som strider mot unionsrätten om skydd av enskilda personers intressen och som

a) har skadat eller sannolikt kommer att skada de kollektiva intressena för enskilda personer som är bosatta i minst två andra medlemsstater än den där

i) handlingen eller underlåtenheten har sitt ursprung eller ägde rum,

ii) den berörda leverantören befinner sig eller är etablerad eller, i tillämpliga fall, dess ombud befinner sig eller är etablerat, eller

iii) spridaren är etablerad, i de fall där överträdelsen begås av spridaren,

b) har orsakat, orsakar eller sannolikt kommer att orsaka skada på enskilda personers kollektiva intressen och uppvisar gemensamma drag, till exempel genom att innebära bruk av samma olagliga metoder eller åsidosättande av samma intresse, samt begås av samma operatör och begås samtidigt i minst tre medlemsstater.

62. kritisk infrastruktur: kritisk infrastruktur enligt definitionen i artikel 2.4 i direktiv (EU) 2022/2557.

63. AI-modell för allmänna ändamål: en AI-modell, även när en sådan AI-modell tränas med en stor mängd data med hjälp av övervakning i stor skala, som uppvisar betydande generalitet och på ett kompetent sätt kan utföra ett brett spektrum av distinkta uppgifter oavsett hur modellen släppts ut på marknaden och som kan integreras i en rad system eller tillämpningar i efterföljande led, utom AI-modeller som används för forsknings-, utvecklings- eller prototypverksamhet innan de släpps ut på marknaden.

64. kapacitet med hög påverkansgrad: kapacitet som motsvarar eller överstiger den kapacitet som registrerats i de mest avancerade AI-modellerna för allmänna ändamål.

65. systemrisk: en risk som specifikt gäller kapaciteten med hög påverkansgrad hos AI-modeller för allmänna ändamål, som påverkar unionsmarknaden i betydande grad på grund av sin räckvidd eller på grund av rimligen förutsägbara negativa effekter på folkhälsa, säkerhet, allmän säkerhet, grundläggande rättigheter och samhället som helhet, och som kan spridas i stor skala i hela värdekedjan.

66. AI-system för allmänna ändamål: ett AI-system som bygger på en AI-modell för allmänna ändamål och med kapacitet för en rad olika ändamål, både för direkt användning och för integrering i andra AI-system.

67. flyttalsberäkning: varje matematisk operation eller tilldelning som inbegriper flyttal, som är en delmängd av de reella talen som typiskt representeras på datorer genom ett heltal med fast precision multiplicerad med en heltalsexponent med en fast talbas.

68. leverantör i efterföljande led: en leverantör av ett AI-system, inbegripet ett AI-system för allmänna ändamål, som integrerar en AI-modell, oavsett om modellen levereras av dem själva och integreras vertikalt eller levereras av en annan enhet på grund av avtalsbestämmelser.

Artikel 4

AI-kunskap

Leverantörer och spridare av AI-system ska vidta åtgärder för att i största möjliga mån säkerställa att deras personal och andra personer som för deras räkning arbetar med drift och användning av AI-system har tillräckliga AI-kunskaper, med beaktande av deras tekniska kunskaper, erfarenhet och utbildning samt det sammanhang i vilket AI-systemen ska användas, och med hänsyn till de personer eller grupper av personer på vilka AI-systemen ska användas.

KAPITEL II
FÖRBJUDNA METODER FÖR ARTIFICIELL INTELLIGENS

Artikel 5

Förbjudna AI-metoder

1. Följande AI-metoder ska vara förbjudna:

a) Utsläppande på marknaden, ibruktagande eller användning av ett AI-system som utnyttjar subliminala tekniker som människor inte är medvetna om ***eller avsiktligt manipulerande eller vilseledande tekniker som syftar eller leder till en*** väsentlig ***snedvridning*** av en persons ***eller en grupp av personers*** beteende ***genom att avsevärt försämra deras förmåga att fatta ett välgrundat beslut, vilket får en person att fatta ett beslut som den inte skulle ha fattat annars,*** på ett sätt som orsakar eller sannolikt kommer att orsaka ***betydande*** skada för den personen, en annan person ***eller en grupp av personer***.

b) Utsläppande på marknaden, ibruktagande eller användning av ett AI-system som utnyttjar någon sårbarhet hos en ***person eller en*** specifik grupp av personer som härrör från ålder, ***funktionsnedsättning eller en specifik social eller ekonomisk situation, med målet eller verkan att*** väsentligt ***snedvrida*** beteendet hos ***den personen eller*** en person som tillhör den gruppen på ett sätt som orsakar eller ***rimligt*** sannolikt kommer att orsaka ***betydande skada*** för den personen eller en annan person.

c) Utsläppande på marknaden, ibruktagande eller användning av AI-system ▌ för utvärdering eller klassificering av ***fysiska personer eller grupper av personer*** under en viss tidsperiod på grundval av deras sociala beteende eller kända, ***uttydda*** eller förutsedda personliga eller personlighetsrelaterade egenskaper, med en social poängsättning som leder till det ena eller båda av följande:

i) Skadlig eller ogynnsam behandling av vissa fysiska personer eller hela grupper av personer i sociala sammanhang ***som*** saknar koppling till de sammanhang i vilka berörda data ursprungligen genererades eller samlades in.

ii) Skadlig eller ogynnsam behandling av vissa fysiska personer eller ▌ grupper av personer som är omotiverad eller oproportionerlig i förhållande till personernas sociala beteende eller till hur allvarligt beteendet är.

d) ***Utsläppande på marknaden, ibruktagande för detta specifika ändamål eller användning av ett AI-system för riskbedömningar av fysiska personer i syfte att bedöma eller förutse sannolikheten för att en fysisk person begår ett brott, uteslutande grundat på profileringen av en fysisk person eller på en bedömning av deras personlighetsdrag och egenskaper; detta förbud ska inte tillämpas på AI-system som används för att stödja mänsklig bedömning av en persons inblandning i brottslig verksamhet, som redan grundas på objektiva och verifierbara fakta med direkt anknytning till brottslig verksamhet.***

e) ***Utsläppande på marknaden, ibruktagande för detta specifika ändamål eller användning av AI-system som skapar eller utvidgar databaser för ansiktsigenkänning genom oriktad skrapning av ansiktsbilder från internet eller övervakningskameror.***

f) Utsläppande på marknaden, ibruktagande för detta specifika ändamål eller användning av AI-system för att uttyda en fysisk persons känslor på arbetsplatsen eller vid utbildningsinstitutioner, såvida inte AI-systemets användning är avsett att införas eller släppas ut på marknaden av medicinska skäl eller säkerhetsskäl.

g) ***Utsläppande på marknaden, ibruktagande för detta specifika ändamål eller användning av system för biometrisk kategorisering som kategoriserar fysiska personer individuellt på grundval av deras biometriska uppgifter för att härleda eller dra slutsatser om en persons ras, politiska åsikter, medlemskap i fackförening, religiösa eller filosofiska övertygelse, sexualliv eller sexuella läggning; detta förbud omfattar inte märkning eller filtrering av lagligen förvärvade biometriska dataset, såsom bilder, grundat på biometriska uppgifter eller kategorisering av biometriska uppgifter på området för brottsbekämpning.***

h) Användning av system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpningsändamål, ▌ såvida inte och endast i den mån sådan användning är absolut nödvändig för något av följande syften:

i) Målinriktad sökning efter specifika ▌ offer för ***människorov, människohandel eller sexuellt utnyttjande av människor, samt sökning efter*** försvunna ***personer***.

ii) Förhindrande av ett specifikt, betydande och överhängande hot mot fysiska personers liv eller fysiska säkerhet eller ***ett verkligt och aktuellt eller verkligt och förutsebart hot*** om en terroristattack.

iii) ▌ Lokalisering ***eller*** identifiering ***av en person som misstänks ha begått ett brott, i syfte att genomföra en*** brotts***utredning, lagföring eller ett verkställande av en straffrättslig påföljd för brott som avses i kapitel II*** och som i den berörda medlemsstaten kan leda till fängelse eller annan frihetsberövande åtgärd under en längsta tidsperiod på minst ***fyra*** år.

▌

Led h i första stycket påverkar inte artikel 9 i förordning (EU) 2016/679 för behandling av biometriska uppgifter för andra ändamål än brottsbekämpning.

2. Användningen av system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpningsändamål för något av de syften som avses i punkt 1 h ska ***införas endast för de ändamål som anges i punkt 1 h för att bekräfta identiteten av den individ som särskilt avses och den ska*** ta hänsyn till följande element:

a) Arten av den situation som ger upphov till den eventuella användningen, särskilt vad gäller hur allvarlig, sannolik och omfattande skadan blir om systemet inte används.

b) Konsekvenserna av användningen av systemet för alla berörda personers rättigheter och friheter, särskilt vad gäller hur allvarliga, sannolika och omfattande dessa konsekvenser är.

Dessutom ska användningen av system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpningsändamål för något av de syften som avses i punkt 1 h i denna artikel vara förenlig med nödvändiga och proportionella skyddsåtgärder och villkor avseende användningen ***i enlighet med nationell lagstiftning som tillåter användning av dessa***, särskilt vad gäller tidsmässiga och geografiska begränsningar samt personbegränsningar. ***Användningen av systemet för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser ska tillåtas endast om den relevanta brottsbekämpande myndigheten har slutfört en konsekvensbedömning avseende grundläggande rättigheter såsom föreskrivs i artikel 27 och har registrerat systemet i EU-databasen i enlighet med artikel 49. I vederbörligen motiverade brådskande fall får dock användningen av sådana system påbörjas utan registrering i EU-databasen, förutsatt att denna registrering slutförs utan onödigt dröjsmål.***

3. Vid tillämpning av punkterna 1 h och 2 ska det för varje ▌ användning för brottsbekämpningsändamål av ett system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser krävas ett förhandstillstånd från en rättslig myndighet eller ▌ en oberoende administrativ myndighet ***vars beslut är bindande*** i den medlemsstat där användningen ska äga rum, utfärdat på motiverad begäran och i enlighet med de närmare bestämmelser i nationell lagstiftning som avses i punkt 5. I vederbörligen motiverade brådskande situationer får dock användningen av ett sådant system påbörjas utan tillstånd, ***förutsatt att ett sådant*** tillstånd begärs ***utan onödigt dröjsmål senast inom 24 timmar***. ***Om ett sådant tillstånd avslås ska användningen stoppas med omedelbar verkan och alla uppgifter samt resultat och utdata som rör denna användning kasseras och raderas.***

Den behöriga rättsliga ***myndigheten eller en oberoende*** administrativ myndighet ***vars beslut är bindande*** ska bevilja tillståndet endast om den, på grundval av objektiva bevis eller tydliga indikationer som lagts fram för den, har förvissat sig om att användningen av det berörda systemet för biometrisk fjärridentifiering i realtid är nödvändig och proportionell för att uppnå ett av de syften som anges i punkt 1 h, i enlighet med vad som anges i begäran ***och i synnerhet förblir begränsad till vad som är strikt nödvändigt när det gäller tidsperioden samt det geografiska tillämpningsområdet och de personer som omfattas***. Vid beslut om begäran ska den ***myndigheten*** beakta de faktorer som avses i punkt 2. ***Inget beslut som har negativa rättsliga följder för en person får fattas enbart på grundval av utdata från systemet för biometrisk fjärridentifiering*** i realtid***.***

4. Utan att det påverkar punkt 3 ska varje användning av ett system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpningsändamål anmälas till den berörda marknadskontrollmyndigheten och den nationella dataskyddsmyndigheten i enlighet med de nationella regler som avses i punkt 5. Anmälan ska åtminstone innehålla den information som specificeras enligt punkt 6 och ska inte inbegripa känsliga operativa uppgifter.

5. En medlemsstat får besluta att föreskriva en möjlighet att helt eller delvis tillåta användning av system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpningsändamål inom de gränser och på de villkor som anges i punkterna 1 h, 2 och 3. ▌ De ***berörda*** medlems***staterna*** ska i ***sin*** nationella lagstiftning fastställa de nödvändiga närmare reglerna för begäran om, utfärdande av och utövande av samt tillsyn över ***och rapportering*** om de tillstånd som avses i punkt 3. I dessa regler ska det också anges för vilka av de syften som förtecknas i punkt 1 h, inbegripet för vilka av de brott som avses i led iii i punkt 1 h, de behöriga myndigheterna kan få tillstånd att använda dessa system för brottsbekämpningsändamål. ***Medlemsstaterna ska till kommissionen anmäla dessa regler senast 30 dagar efter deras antagande. Medlemsstaterna får införa mer restriktiva lagar om användningen av system för biometrisk fjärridentifiering i enlighet med unionsrätten.***

6. Medlemsstaternas nationella marknadskontrollmyndigheter och nationella dataskyddsmyndigheter som har underrättats om användningen av system för biometrisk fjärridentifiering i realtid på allmänt tillgänglig plats för brottsbekämpande ändamål i enlighet med punkt 4 bör lämna in årliga rapporter till kommissionen om sådan användning. För detta ändamål ska kommissionen förse medlemsstaterna och de nationella marknadskontrollmyndigheterna och dataskyddsmyndigheterna med en mall som inbegriper information om antalet beslut som fattats av behöriga rättsliga myndigheter eller en oberoende administrativ myndighet vars beslut är bindande gällande ansökningar om tillstånd i enlighet med punkt 3 och utkomsten av dessa.

7. Kommissionen ska offentliggöra årliga rapporter om användningen av system för biometrisk fjärridentifiering i realtid på allmänt tillgänglig plats för brottsbekämpande ändamål på grundval av aggregerade data från medlemsstaterna baserat på de årliga rapporter som avses i punkt 6. Dessa årsrapporter ska inte omfatta känsliga operativa uppgifter som rör relaterad brottsbekämpande verksamhet.

8. Denna artikel ska inte påverka de förbud som gäller när en praxis för artificiell intelligens strider mot annan unionsrätt.

KAPITEL III
AI-SYSTEM MED HÖG RISK

Avsnitt 1
Klassificering av AI-system som högrisksystem

Artikel 6

Klassificeringsregler för AI-system med hög risk

1. Oaktat att ett AI-system släpps ut på marknaden eller tas i bruk oberoende av de produkter som avses i leden a och b ska detta AI-system betraktas som högrisksystem om båda följande villkor är uppfyllda:

   a) AI-systemet är avsett att användas som en säkerhetskomponent i en produkt, eller ***AI-systemet*** är i sig en produkt, som omfattas av unionens harmoniseringslagstiftning enligt förteckningen i bilaga I.

   b) Den produkt vars säkerhetskomponent ***enligt led a*** är AI-systemet, eller själva AI-systemet som en produkt, måste genomgå en tredjepartsbedömning av överensstämmelse för att den produkten ska kunna släppas ut på marknaden eller tas i bruk i enlighet med den unionslagstiftning om harmonisering som förtecknas i bilaga I.

2. Utöver de AI-system med hög risk som avses i punkt 1 ska AI-system som avses i bilaga III också betraktas som högrisksystem.

3. Genom undantag från punkt 2 ska ett AI-system inte betraktas som högrisksystem om det inte utgör en betydande risk för skada på fysiska personers hälsa, säkerhet eller grundläggande rättigheter, inbegripet genom att det inte väsentligt påverkar resultatet av beslutsfattandet. Detta ska vara fallet om ett eller flera av följande villkor är uppfyllda:

a) AI-systemet är avsett att utföra en snäv processuell uppgift,

b) AI-systemet är avsett att förbättra resultatet av tidigare fullbordad mänsklig verksamhet,

c) AI-systemet är avsett att upptäcka beslutsmönster eller avvikelser från tidigare beslutsmönster och är inte avsett att ersätta eller påverka tidigare slutförd mänsklig bedömning eller

d) AI-systemet är avsett att utföra en förberedande uppgift som är relevant för de användningsfall som förtecknas i bilaga III.

Utan hinder av första stycket ska ett AI-system som avses i bilaga III alltid anses utgöra högrisksystem om AI-systemet utför profilering av fysiska personer.

4. En leverantör som anser att ett AI-system som avses i bilaga III inte är förenat med hög risk ska upprätta dokumentation för sin bedömning innan systemet släpps ut på marknaden eller tas i bruk. Sådana leverantörer ska omfattas av de registreringsskyldigheter som föreskrivs i artikel 49.2. På begäran av nationella behöriga myndigheter ska leverantören tillhandahålla dokumentation som legat till grund för bedömningen.

5. Efter samråd med den europeiska nämnden för artificiell intelligens (nämnden) ska kommissionen senast den ... [18 månader från och med den dag då denna förordning träder i kraft] ge riktlinjer som specificerar det praktiska genomförandet av denna artikel i överensstämmelse med artikel 96, och som innefattar en omfattande förteckning över praktiska exempel på användningsfall av AI-system med och utan hög risk.

6. Kommissionen ska anta delegerade akter i enlighet med artikel 97 i syfte att ändra villkoren i punkt 3 första stycket i denna artikel.

Kommissionen kan anta delegerade akter i enlighet med artikel 97 i syfte att lägga till nya villkor utöver dem som föreskrivs i punkt 3 första stycket eller ändra dem endast om det finns konkreta och tillförlitliga bevis på förekomst av AI-system som omfattas av tillämpningsområdet för bilaga III men som inte utgör en betydande risk för skada på fysiska personers hälsa, säkerhet eller grundläggande rättigheter.

Kommissionen ska anta delegerade akter i enlighet med artikel 97 i syfte att stryka något av de villkor som föreskrivs i punkt 3 första stycket om det finns konkreta och tillförlitliga bevis för att detta är nödvändigt för att upprätthålla skyddsnivån för hälsa, säkerhet och grundläggande rättigheter i unionen.

Eventuella ändringar av villkoren i punkt 3 första stycket ska inte sänka den allmänna skyddsnivån för hälsa, säkerhet och grundläggande rättigheter i unionen.

När kommissionen antar delegerade akter ska den säkerställa överensstämmelse med de delegerade akter som antagits enligt artikel 7.1 och ta hänsyn till marknadsutvecklingen och den tekniska utvecklingen.

Artikel 7

Ändringar av bilaga III

1. Kommissionen ska anta delegerade akter i enlighet med artikel 97 med avseende på att ***ändra*** bilaga III genom att lägga till ***eller ändra användningsfall*** för AI-system med hög risk om båda följande villkor är uppfyllda:

   a) AI-systemen är avsedda att användas inom något av de områden som förtecknas i bilaga III.

b) AI-systemen utgör en risk för skada på hälsa och säkerhet, eller för ▌ negativ inverkan på grundläggande rättigheter, ***och denna risk är*** likvärdig med eller större än den risk för skada eller negativ inverkan som förorsakas av de AI-system med hög risk som redan nämns i bilaga III.

2. Vid bedömningen av villkoret i punkt 1 b ska kommissionen beakta följande kriterier:

a) Det avsedda ändamålet med AI-systemet.

b) I vilken utsträckning ett AI-system har använts eller sannolikt kommer att användas.

c) Typen och mängden data som behandlas och används av AI-systemet, i synnerhet huruvida särskilda kategorier av personuppgifter behandlas.

d) I vilken utsträckning AI-systemet agerar självständigt och det är möjligt för en människa att åsidosätta ett beslut eller rekommendationer som kan leda till potentiell skada.

e) I vilken utsträckning användningen av ett AI-system redan har orsakat skada på hälsa och säkerhet, ▌ ***har haft*** negativ inverkan på de grundläggande rättigheterna eller har gett upphov till betydande farhågor när det gäller ***sannolikheten*** för sådan skada eller negativ inverkan, vilket ***till exempel*** framgår av rapporter eller dokumenterade anklagelser som lämnats till nationella behöriga myndigheter, ***eller, i förekommande fall, av andra rapporter.***

f) Den potentiella omfattningen av sådan skada eller sådan negativ inverkan, särskilt i fråga om intensitet och förmåga att påverka en stor mängd personer ***eller att i oproportionerlig utsträckning påverka en viss grupp av personer.***

g) I vilken utsträckning potentiellt skadade eller negativt påverkade personer är beroende av det resultat som producerats med ett AI-system, särskilt eftersom det av praktiska eller juridiska skäl inte rimligen är möjligt att undantas från detta resultat.

h) I vilken utsträckning ***det föreligger en obalans i fråga om makt, eller*** potentiellt skadade eller negativt påverkade ***personer*** befinner sig i ett utsatt läge i förhållande till spridaren av ett AI-system, särskilt på grund av ***status, auktoritet,*** kunskap, ekonomiska eller sociala omständigheter eller ålder.

i) I vilken utsträckning det resultat som produceras med ***medverkan*** av ett AI-system är lätt att ***korrigera eller*** upphäva, ***med beaktande av tillgängliga tekniska lösningar som möjliggör dess korrigering eller upphävande***, varvid resultat ▌ med en ***negativ*** påverkan på ▌ hälsa, säkerhet e***ller grundläggande rättigheter*** inte ska anses vara lätta att ***korrigera eller*** upphäva.

j) Omfattningen av och sannolikheten för nyttan med användningen av AI-systemet för enskilda personer, grupper eller samhället i stort, inbegripet eventuella förbättringar av produktsäkerheten.

k) I vilken utsträckning befintlig unionsrätt föreskriver

i) effektiva åtgärder för rättslig prövning med hänsyn till de risker som ett AI-system medför, med undantag för skadeståndsanspråk,

ii) effektiva åtgärder för att förebygga eller avsevärt minimera dessa risker.

3. Kommissionen ska anta delegerade akter i enlighet med artikel 97 med avseende på att ändra förteckningen i bilaga III genom att låta AI-system med hög risk utgå om båda följande villkor är uppfyllda:

a) Det berörda AI-systemet medför inte längre någon betydande risk för grundläggande rättigheter, hälsa eller säkerhet, med beaktande av kriterierna i punkt 2.

b) Strykningen sänker inte den övergripande nivån på skyddet för hälsa, säkerhet och grundläggande rättigheter enligt unionsrätten.

Avsnitt 2

Krav på AI-system med hög risk

Artikel 8

Förenlighet med kraven

1. AI-system med hög risk ska uppfylla kraven i detta avsnitt, ***med beaktande av deras avsedda ändamål s****amt den allmänt erkända bästa tekniken inom AI och AI-tillhörande teknik. Det riskhanteringssystem som avses i artikel 9 ska beaktas när förenligheten med dessa krav säkerställs.*

2. Om en produkt innehåller ett AI-system som omfattas av kraven i denna förordning och kraven i unionens harmoniseringslagstiftning i förteckningen i avsnitt A i bilaga I, ska leverantörer ansvara för att säkerställa att deras produkt uppfyller alla tillämpliga krav som uppställs i tillämplig unionsharmoniseringslagstiftning. Vid säkerställandet av att AI-system med hög risk som avses i punkt 1 överensstämmer med kraven i detta avsnitt, och för att säkerställa enhetlighet, motverka dubbelarbete och minimera ytterligare bördor, ska leverantörer kunna välja att, beroende på vad som är lämpligt, integrera de nödvändiga test- och rapporteringsprocesserna, den information och den dokumentation som de tillhandahåller med avseende på sin produkt i dokumentation och förfaranden som redan finns och som krävs enligt den unionsharmoniseringslagstiftning som förtecknas i avsnitt A i bilaga I.

Artikel 9

Riskhanteringssystem

1. Ett riskhanteringssystem ska inrättas, genomföras, dokumenteras och underhållas för AI-system med hög risk.

2. Riskhanteringssystemet ska ***förstås som*** en kontinuerlig iterativ process som ***planeras och*** löper under hela livscykeln för ett AI-system med hög risk, med krav på regelbunden och systematisk ***översyn och*** uppdatering. Det ska innehålla följande steg:

   a) Identifiering och analys av de kända och ***rimligen*** förutsebara risker ***som AI-systemet med hög risk kan medföra för hälsa, säkerhet och grundläggande rättigheter när*** AI-systemet med hög risk ***används i enlighet med sitt avsedda ändamål.***

   b) Uppskattning och utvärdering av de risker som kan uppstå när AI-systemet med hög risk används i enlighet med dess avsedda ändamål och under förhållanden där det kan förekomma rimligen förutsebar felaktig användning.

   c) Utvärdering av andra risker som eventuellt kan uppstå på grundval av en analys av data som samlats in från det system för övervakning efter utsläppande på marknaden som avses i artikel 72.

   d) Antagande av ***lämpliga och riktade*** riskhanteringsåtgärder ***utformade för att hantera de risker som identifierats enligt led a***.

3. ***De risker som avses i denna*** artikel ***ska endast avse de risker som rimligen kan begränsas eller elimineras genom utveckling eller utformning av AI-systemet med hög risk eller tillhandahållande av adekvat teknisk information.***

4. I de riskhanteringsåtgärder som avses i punkt 2 d ska vederbörlig hänsyn tas till de effekter och den möjliga ***interaktion*** som följer av den kombinerade tillämpningen av kraven i detta avsnitt, ***i syfte att minimera riskerna mer effektivt och samtidigt uppnå en lämplig balans i genomförandet av åtgärderna för att uppfylla dessa krav.***

5. De riskhanteringsåtgärder som avses i punkt 2 d ska vara sådana att ***relevanta*** kvarvarande risker förknippade med varje fara samt den totala kvarvarande risken i AI-systemen med hög risk bedöms ***vara acceptabla***.

   Vid fastställandet av de lämpligaste riskhanteringsåtgärderna ska följande säkerställas:

   a) Eliminering eller minskning av risker som ***identifierats och utvärderats i enlighet med punkt 2*** så långt som ***tekniskt möjligt*** genom lämplig konstruktion och utveckling ***av AI-systemet med hög risk.***

   b) När det är lämpligt, genomförande av lämpliga begränsnings- och kontrollåtgärder för att ***bemästra*** risker som inte kan elimineras.

   c) Tillhandahållande av ***erforderlig*** information enligt artikel 13 och, i förekommande fall, utbildning för ***spridare***. ▌

För att eliminera eller minska risker i samband med användningen av AI-systemet med hög risk ska vederbörlig hänsyn tas till den tekniska kunskap, erfarenhet och utbildning som ***spridaren*** förväntas ha och det ***förmodade sammanhang*** i vilket systemet är avsett att användas.

6. AI-system med hög risk ska testas i syfte att identifiera de lämpligaste ***och bäst riktade*** riskhanteringsåtgärderna. Testerna ska säkerställa att AI-system med hög risk fungerar konsekvent för sitt avsedda ändamål och att de uppfyller kraven i detta avsnitt.

7. Testningsförfarandena ***får omfatta testning under verkliga förhållanden i enlighet med artikel 60***.

8. Testning av AI-systemen med hög risk ska utföras, beroende på vad som är lämpligt, när som helst under hela utvecklingsprocessen och i alla händelser innan de släpps ut på marknaden eller tas i bruk. Testning ska utföras på grundval av ***i förväg*** definierade mått och sannolikhetsgränser som är lämpliga för det avsedda ändamålet med AI-systemet med hög risk.

9. Vid genomförandet av det riskhanteringssystem som föreskrivs i punkterna 1–7 ***ska leverantörer ta*** hänsyn till ***huruvida*** AI-systemet med hög risk, ***med tanke på dess avsedda ändamål,*** sannolikt kommer att ha en ***negativ påverkan på personer som är yngre än 18 år och, i förekommande fall, andra grupper av utsatta personer.***

10. För ***leverantörer av AI-system med hög risk som omfattas av krav avseende interna riskhanteringsprocesser enligt andra relevanta unionsrättsliga bestämmelser får*** de aspekter som regleras i punkterna 1–9 ingå i, ***eller kombineras med,*** de riskhanteringsförfaranden som fastställs i ▌ enlighet med ***den lagstiftningen***.

Artikel 10

Data och dataförvaltning

1. AI-system med hög risk som använder teknik som inbegriper träning av AI-modeller med data ska utvecklas på grundval av tränings-, validerings- och testdataset som uppfyller de kvalitetskriterier som avses i punkterna 2–5 ***när sådana dataset används***.

2. Tränings-, validerings- och testdataset ska omfattas av metoder för dataförvaltning och datahantering ***som är lämpliga för det avsedda ändamålet med AI-systemet med hög risk***. Dessa metoder ska särskilt avse

   a) relevanta utformningsval,

   b) datainsamlingsprocesser och uppgifternas ursprung samt, när det gäller personuppgifter, datainsamlingens ursprungliga ändamål,

   ▌

c) relevanta åtgärder för datapreparering, såsom annotation, märkning, uppstädning, ***uppdatering***, förädling och aggregering,

d) formulering av ▌ antaganden, särskilt när det gäller den information som berörda data förväntas beskriva och representera,

e) ***en*** bedömning av tillgängligheten, mängden och lämpligheten avseende de dataset som behövs,

f) undersökning med avseende på eventuella snedvridningar ***som sannolikt kommer att påverka människors hälsa och säkerhet, inverka negativt på de grundläggande rättigheterna eller leda till diskriminering som är förbjuden enligt unionsrätten, särskilt när utdata påverkar indata för framtida drift***,

g) lämpliga åtgärder för att upptäcka, förebygga och begränsa eventuella snedvridningar som identifierats enligt led f,

h) identifiering av ***relevanta*** dataluckor eller brister ***som hindrar efterlevnad av denna förordning***, och hur dessa luckor och brister kan åtgärdas.

3. Tränings-, validerings- och test***dataset*** ska vara relevanta, ***tillräckligt*** representativa, ***och så långt som möjligt*** felfria och fullständiga ***i förhållande till det avsedda ändamålet.*** De ska ha lämpliga statistiska egenskaper, däribland, i förekommande fall, vad gäller de personer eller grupper av personer ***med avseende på vilka*** AI-systemet med hög risk är avsett att användas. Egenskaperna hos dessa dataset kan uppfyllas på nivån för enskilda dataset eller på nivån av en kombination av dessa.

4. ***Dataseten*** ska beakta, i den mån som krävs på grund av det avsedda ändamålet, de egenskaper eller element som är utmärkande för just den specifika geografiska, ***kontextuella,*** beteendemässiga eller funktionsmässiga situation där AI-systemet med hög risk är avsett att användas.

5. I den utsträckning det är absolut nödvändigt för att säkerställa ▌ upptäckt och korrigering av snedvridning i samband med AI-systemen med hög risk, ***i enlighet med punkt 2, led f och g i denna artikel*** får leverantörer av sådana system ***undantagsvis*** behandla särskilda kategorier av personuppgifter, med förbehåll för lämpliga skyddsåtgärder för fysiska personers grundläggande rättigheter och friheter. ***Utöver bestämmelserna i förordning (EU) 2016/679, direktiv (EU) 2016/680 och förordning (EU) 2018/1725 ska samtliga följande villkor gälla för att sådan behandling ska kunna äga rum:***

   a) Upptäckt och korrigering av snedvridning kan inte uppnås på ett effektivt sätt genom behandling av andra data, inbegripet syntetiska eller anonymiserade data.

b) De särskilda kategorierna av personuppgifter omfattas av tekniska begränsningar för vidareutnyttjande av personuppgifter samt säkerhetsåtgärder och integritetsbevarande åtgärder på aktuell teknisk nivå, inbegripet pseudonymisering.

c) De särskilda kategorierna av personuppgifter omfattas av åtgärder för att säkerställa att de personuppgifter som behandlas är säkra, skyddade, omfattas av lämpliga skyddsåtgärder, inbegripet strikta kontroller och dokumentation av åtkomsten, för att undvika missbruk och säkerställa att endast behöriga personer har tillgång till dessa personuppgifter genom lämpliga konfidentialitetskrav.

d) De särskilda kategorierna av personuppgifter får inte översändas, överföras eller på annat sätt göras tillgängliga för andra parter.

e) De särskilda kategorierna av personuppgifter raderas när snedvridningen har korrigerats eller personuppgifternas lagringstid har löpt ut, beroende på vilket som inträffar först.

f) Registren över behandling enligt förordningarna (EU) 2016/679 och (EU) 2018/1725 och direktiv (EU) 2016/680 innehåller skälen till varför behandlingen av särskilda kategorier av personuppgifter var absolut nödvändig för att upptäcka och korrigera snedvridningar och varför detta mål inte kunde uppnås genom behandling av andra data.

6. För utvecklingen av AI-system med hög risk som ***inte använder*** teknik som inbegriper träning av AI-modeller tillämpas ***punkterna 2–5 endast på testdataset***.

Artikel 11

Teknisk dokumentation

1. Den tekniska dokumentationen för ett AI-system med hög risk ska upprättas innan systemet släpps ut på marknaden eller tas i bruk och ska hållas uppdaterad.

Den tekniska dokumentationen ska upprättas på ett sådant sätt att det visas att AI-systemet med hög risk är förenligt med kraven i detta avsnitt, och så att nationella behöriga myndigheter och anmälda organ får den information som krävs ***i klar och begriplig form*** för att bedöma om AI-systemet uppfyller dessa krav. Den ska minst innehålla de delar som anges i bilaga IV. ***Små och medelstora företag, inbegripet nystartade företag, får tillhandahålla de delar av den tekniska dokumentation som anges i bilaga IV på ett förenklat sätt. För detta ändamål ska kommissionen upprätta ett förenklat formulär för teknisk dokumentation som är inriktat på små företags och mikroföretags behov. Om ett litet eller medelstort företag, inbegripet ett nystartat företag, väljer att tillhandahålla den information som krävs enligt bilaga IV på ett förenklat sätt ska det använda det formulär som avses i denna punkt. Anmälda organ ska godta formuläret för bedömning av överensstämmelse.***

2. Om ett AI-system med hög risk som är kopplat till en produkt, som omfattas av den unionslagstiftning om harmonisering som förtecknas i avsnitt A i bilaga I, släpps ut på marknaden eller tas i bruk ska en enda teknisk uppsättning dokumentation upprättas som innehåller all den information som anges i ***punkt 1*** samt den information som krävs enligt dessa rättsakter.

3. Kommissionen ska anta delegerade akter i enlighet med artikel 97 med avseende på att ändra bilaga IV när så krävs för att säkerställa att den tekniska dokumentationen, mot bakgrund av den tekniska utvecklingen, innehåller all information som krävs för att bedöma systemets förenlighet med kraven i detta avsnitt.

Artikel 12

Arkivering

1. AI-system med hög risk ska ***tekniskt möjliggöra*** automatisk registrering av händelser (loggar) ***under hela deras livstid.***

2. ***För att*** säkerställa en spårbarhetsnivå för AI-högrisksystemets funktion ▌ som är lämplig för systemets avsedda ändamål ska ***loggningskapaciteten möjliggöra registrering av händelser som är relevanta för***

   a) identifiering av situationer som kan resultera i att AI-högrisksystemet utgör en risk i den mening som avses i artikel 79.1 eller i en väsentlig ändring,

   b) underlättande av den övervakning efter utsläppande på marknaden som avses i artikel 72 och

   c) övervakning av driften av AI-system med hög risk som avses i artikel 26.6.

▌

3. För AI-system med hög risk som avses i punkt 1 a i bilaga III ska loggningsfunktionerna åtminstone tillhandahålla följande:

   a) Registrering av perioden för varje användning av systemet (startdatum och starttidpunkt samt slutdatum och sluttidpunkt för varje användning).

   b) Den referensdatabas mot vilken indata har kontrollerats av systemet.

c) Indata för vilka sökningen har lett till en träff.

d) Identifiering av de fysiska personer som deltar i kontrollen av resultaten enligt artikel 14.5.

Artikel 13

Transparens och tillhandahållande av information till ***spridare***

1. AI-system med hög risk ska utformas och utvecklas på ett sådant sätt att driften av dem är tillräckligt transparent för att ***spridare*** ska kunna tolka systemets utdata och använda dem på lämpligt sätt. En lämplig typ och grad av transparens ska säkerställas, ▌ i syfte att uppnå uppfyllelse av ***leverantörens och spridarens*** relevanta skyldigheter enligt avsnitt 3.

2. AI-system med hög risk ska åtföljas av en bruksanvisning i ett lämpligt digitalt eller annat format som inbegriper kortfattad, fullständig, korrekt och tydlig information som är relevant, tillgänglig och begriplig för spridare.

3. ***Bruksanvisningen ska minst innehålla följande information:***

a) Namn och kontaktuppgifter för leverantören och i tillämpliga fall för dennes ombud.

b) Egenskaperna, kapaciteten och prestandabegränsningarna hos AI-systemet med hög risk, inbegripet

i) dess avsedda ändamål,

ii) den nivå avseende noggrannhet, ***inbegripet mätningarna av denna,*** robusthet och cybersäkerhet som avses i artikel 15 mot vilken AI-systemet med hög risk har testats och validerats och som kan förväntas, samt alla kända och förutsebara omständigheter som kan påverka den förväntade noggrannhets-, robusthets- och cybersäkerhetsnivån,

iii) varje känd eller förutsebar omständighet, som har samband med användningen av AI-systemet med hög risk i enlighet med dess avsedda ändamål eller under förhållanden där det kan förekomma rimligen förutsebar felaktig användning, som kan leda till risker för hälsa och säkerhet eller grundläggande rättigheter ***som avses i artikel 9.2***,

iv) i tillämpliga fall, den tekniska kapaciteten och de tekniska egenskaperna hos AI-systemet med hög risk ***att tillhandahålla information som är relevant för att förklara dess utdata,***

v) ***i lämpliga fall,*** dess prestanda ***vad gäller specifika*** personer eller grupper av personer som omfattas av den avsedda användningen av systemet,

vi) i tillämpliga fall, specifikationer för indata, eller all annan relevant information i fråga om de tränings-, validerings- och testdataset som används, med beaktande av AI-högrisksystemets avsedda ändamål.

vii) i tillämpliga fall, information som gör det möjligt för spridare att tolka utdata från AI-systemet med hög risk och använda dem på lämpligt sätt.

c) Eventuella ändringar av AI-systemet med hög risk och dess prestanda som leverantören på förhand har fastställt vid tidpunkten för den inledande bedömningen av överensstämmelse.

d) De åtgärder för mänsklig tillsyn som avses i artikel 14, inbegripet de tekniska åtgärder som införts för att underlätta ***spridarnas*** tolkning av AI-högrisksystemens utdata.

e) ***De data- och maskinvaruresurser som krävs***, den förväntade livslängden för AI-systemet med hög risk och alla nödvändiga underhålls- och omsorgsåtgärder, i***nbegripet deras frekvens,*** för att säkerställa att AI-systemet fungerar korrekt, även när det gäller programvaruuppdateringar.

f) I förekommande fall, en beskrivning av de mekanismer som ingår i AI-högrisk***systemet som gör det möjligt*** för spridarna ***att korrekt samla in, lagra och tolka loggarna i enlighet med artikel 12.***

Artikel 14

Mänsklig tillsyn

1. AI-system med hög risk ska utformas och utvecklas på ett sådant sätt, inbegripet med lämpliga verktyg för människa–maskin-gränssnitt, att fysiska personer på ett effektivt sätt kan ha tillsyn över dem när de används.

2. Mänsklig tillsyn ska syfta till att förebygga eller minimera de risker för hälsa, säkerhet eller grundläggande rättigheter som kan uppstå när ett AI-system med hög risk används i enlighet med sitt avsedda ändamål eller under förhållanden där det kan förekomma rimligen förutsebar felaktig användning, särskilt när sådana risker kvarstår trots tillämpningen av andra krav i detta avsnitt.

3. Tillsyns***åtgärderna ska stå i proportion till riskerna, graden av autonomi och användningssammanhang för AI-systemet*** med hög risk, ***och*** ska säkerställas genom en eller båda av följande ***typer av*** åtgärder:

   a) ***Åtgärder*** som leverantören har fastställt och, när det är tekniskt möjligt, byggt in i AI-systemet med hög risk innan det släpps ut på marknaden eller tas i bruk.

   b) ***Åtgärder*** som leverantörer har fastställt innan AI-systemet med hög risk släpps ut på marknaden eller tas i bruk och som är lämpliga att genomföras av spridaren.

4. ***Vid genomförandet av punkterna 1,2 och 3*** ska ***AI-systemet med hög risk tillhandahållas användaren på ett sådant sätt att fysiska personer*** som fått i uppdrag att ombesörja mänsklig tillsyn ***ges möjlighet*** att på lämpligt sätt ***och i proportion till*** följande omständigheter:

   a) ***Korrekt*** förstå den ***relevanta*** kapaciteten och begränsningarna hos AI-systemet med hög risk och på vederbörligt sätt kunna övervaka dess drift, bland annat ***i syfte att upptäcka och ta itu med*** avvikelser, funktionsstörningar och oväntad prestanda ▌.

   b) Förbli medvetna om den möjliga tendensen att automatiskt eller i alltför hög grad lita på de utdata som produceras av ett AI-system med hög risk (”automationssnedvridning”, ”automation bias”), särskilt när det gäller AI-system med hög risk som används för att tillhandahålla information eller rekommendationer för beslut som ska fattas av fysiska personer.

   c) ▌Korrekt kunna tolka utdata från AI-systemet med hög risk, med beaktande av ***till exempel*** tillgängliga tolkningsverktyg och tolkningsmetoder.

   d) ▌I vissa situationer besluta att inte använda AI-systemet med hög risk eller på annat sätt bortse från, åsidosätta eller reversera de resultat som AI-systemet med hög risk genererar.

   e) ▌Ingripa i driften av AI-systemet med hög risk eller stoppa systemet med en ”***stopp***knapp” eller ett liknande förfarande s***om gör det möjligt för systemet att stoppas i ett säkert läge.***

5. För AI-system med hög risk som avses i punkt 1 a i bilaga III ska de åtgärder som avses i punkt 3 i denna artikel dessutom vara sådana att de säkerställer att ingen åtgärd och inget beslut vidtas respektive fattas av ***spridaren*** på grundval av den identifiering som systemet resulterar i, såvida inte denna identifiering har kontrollerats och bekräftats ***separat*** av minst två fysiska personer ***med nödvändig kompetens, utbildning och auktoritet.***

Kravet på en separat kontroll av minst två fysiska personer ska inte tillämpas på AI-system med hög risk som används inom områdena brottsbekämpning, migration, gränskontroll eller asyl, där en tillämpning av detta krav enligt unionsrätten eller nationell rätt skulle betraktas som oproportionell.

Artikel 15

Noggrannhet, robusthet och cybersäkerhet

1. AI-system med hög risk ska utformas och utvecklas på ett sådant sätt att de ▌ uppnår en lämplig nivå avseende noggrannhet, robusthet och cybersäkerhet och presterar väl i dessa avseenden under hela sin livscykel.

2. För att hantera de tekniska aspekterna av hur man mäter de lämpliga nivåer av noggrannhet och robusthet som anges i punkt 1 och andra relevanta prestandamått ska kommissionen i samarbete med relevanta berörda parter och organisationer, såsom metrologi- och riktmärkningsmyndigheter, vid behov, uppmuntra utvecklingen av riktmärken och mätmetoder.

3. Noggrannhetsnivåerna och relevanta noggrannhetsmått för AI-system med hög risk ska anges i de medföljande bruksanvisningarna.

4. AI-system med hög risk ska vara ***så*** resilienta ***som möjligt mot*** felaktigheter, funktionsfel eller inkonsekvenser som kan uppstå inom det system eller den miljö där systemet är i drift, särskilt på grund av deras interaktion med fysiska personer eller andra system. ***Tekniska och organisatoriska åtgärder ska vidtas i detta avseende.***

   Robustheten hos AI-system med hög risk kan uppnås genom lösningar med teknisk redundans, som kan omfatta backup eller felsäkra planer.

   AI-system med hög risk som fortsätter att lära sig efter det att de har släppts ut på marknaden eller tagits i bruk ska utvecklas på ett sådant sätt att ***risken för att eventuellt snedvridna utdata påverkar*** indata för framtida drift (”återföring”) ***elimineras eller minskas så mycket som möjligt*** och så att det säkerställs att sådan återföring hanteras på vederbörligt sätt med lämpliga kompenserande åtgärder.

5. AI-system med hög risk ska vara resilienta mot försök av obehöriga tredje parter att ändra sin användning, ***utdata*** eller prestanda genom att utnyttja systemets sårbarheter.

De tekniska lösningar som syftar till att säkerställa cybersäkerhet i AI-system med hög risk ska vara anpassade till de relevanta omständigheterna och riskerna.

De tekniska lösningarna för att hantera AI-specifika sårbarheter ska, när det är lämpligt, inbegripa åtgärder för att förebygga, ***upptäcka***, ***reagera på, åtgärda*** och bekämpa attacker som försöker manipulera träningsdatasetet (”dataförgiftning”) ***eller förtränade komponenter som används i träningen (”modellförgiftning”)***, indata som är utformade för att få AI-modellen att göra ett misstag (”antagonistiska exempel” ***eller*** ”***modellkringgående***”), ***sekretessangrepp*** eller modellfel.

Avsnitt 3

Skyldigheter för leverantörer och *spridare* av AI-system med hög risk samt andra parter

Artikel 16

Skyldigheter för leverantörer av AI-system med hög risk

Leverantörer av AI-system med hög risk ska

a) säkerställa att deras AI-system med hög risk uppfyller kraven i avsnitt 2,

b) ***på AI-systemet med hög risk eller, om detta inte är möjligt, på dess förpackning eller i dess åtföljande dokumentation, beroende på vad som är tillämpligt, ange deras namn, registrerat firmanamn eller registrerat varumärke, den adress där de kan kontaktas,***

c) ha ett kvalitetsstyrningssystem som uppfyller kraven i artikel 17,

d) ***förvara den*** dokumentation ***som avses i artikel 18,***

e) spara de loggar som genereras automatiskt av deras AI-system med hög risk ***enligt artikel 19***, när loggarna står under deras kontroll,

f) säkerställa att AI-systemet med hög risk genomgår det relevanta förfarande för bedömning av överensstämmelse ***som avses i artikel 43*** innan det släpps ut på marknaden eller tas i bruk,

g) utarbeta en EU-försäkran om överensstämmelse i enlighet med artikel 47,

h) anbringa CE-märkningen på AI-systemet med hög risk eller, om detta inte är möjligt, på dess förpackning eller i dess åtföljande dokumentation, för att påvisa överensstämmelse med denna förordning i enlighet med artikel 48,

i) fullgöra de registreringsskyldigheter som avses i artikel 49***.1***,

j) vidta nödvändiga korrigerande åtgärder ***och tillhandahålla den information som krävs enligt artikel 20,***

k) på ***motiverad*** begäran av en nationell behörig myndighet visa att AI-systemet med hög risk uppfyller kraven i avsnitt 2,

l) säkerställa att AI-systemet med hög risk uppfyller tillgänglighetskraven i enlighet med direktiven (EU) 2016/2102 och (EU) 2019/882.

Artikel 17

Kvalitetsstyrningssystem

1. Leverantörer av AI-system med hög risk ska inrätta ett kvalitetsstyrningssystem som säkerställer efterlevnad av denna förordning. Systemet ska dokumenteras på ett systematiskt och ordnat sätt i form av skriftliga riktlinjer, förfaranden och instruktioner och ska omfatta åtminstone följande aspekter:

   a) En strategi för efterlevnad av regelverket, inklusive efterlevnad av förfaranden för bedömning av överensstämmelse och för hantering av ändringar av AI-systemet med hög risk.

   b) Tekniker, förfaranden och systematiska åtgärder som ska användas för utformning av AI-systemet med hög risk samt för kontroll och verifikation för utformningen.

   c) Tekniker, förfaranden och systematiska åtgärder som ska användas för utveckling, kvalitetskontroll och kvalitetssäkring av AI-systemet med hög risk.

   d) Undersöknings-, test- och valideringsförfaranden som ska utföras före, under och efter utvecklingen av AI-systemet med hög risk och hur ofta de ska utföras.

e) Tekniska specifikationer, inbegripet standarder, som ska tillämpas och, om de relevanta harmoniserade standarderna inte tillämpas fullt ut, ***eller inte omfattar alla relevanta krav i avsnitt 2***, de medel som ska användas för att säkerställa att AI-systemet med hög risk uppfyller ***dessa*** krav ▌.

f) System och förfaranden för datahantering, inbegripet data***fångst, data***insamling, dataanalys, datamärkning, datalagring, datafiltrering, datautvinning, dataaggregering, lagring av uppgifter och varje annan åtgärd som avser data och som utförs före och för utsläppandet på marknaden eller ibruktagandet av AI-system med hög risk.

g) Det riskhanteringssystem som avses i artikel 9.

h) Upprättande, genomförande och underhåll av ett system för övervakning efter utsläppande på marknaden i enlighet med artikel 72.

i) Förfaranden som berör rapportering av ***en allvarlig incident*** i enlighet med artikel 73.

j) Hantering av kommunikation med nationella behöriga myndigheter, ***andra relevanta*** myndigheter, inbegripet ***de*** som tillhandahåller eller stöder tillgången till uppgifter, anmälda organ, andra operatörer, kunder eller andra berörda parter.

k) System och förfaranden för arkivering av all relevant dokumentation och information.

l) Resurshantering, inbegripet åtgärder som berör försörjningstrygghet.

m) En ram för ansvarsutkrävande som fastställer ledningens och övrig personals ansvar vad gäller samtliga aspekter som anges i denna punkt.

2. Genomförandet av de aspekter som avses i punkt 1 ska stå i proportion till storleken på leverantörens organisation. ***Leverantörerna ska i alla händelser iaktta den grad av noggrannhet och den skyddsnivå som krävs för att säkerställa att deras AI-system med hög risk står i överensstämmelse med denna förordning.***

3. Leverantörer av AI-system med hög risk som omfattas av skyldigheter avseende kvalitetsstyrningssystem eller en likvärdig funktion enligt relevant sektorsspecifik unionsrätt får inkludera de aspekter som anges i punkt 1 i de kvalitetsstyrningssystem som fastställs i enlighet med den lagstiftningen.

4. För leverantörer som är ***finans***institut ***som omfattas av krav avseende interna styrelseformer, arrangemang eller processer enligt unionsrätten om finansiella tjänster*** ska skyldigheten att ***införa*** ett kvalitetsstyrningssystem, ***med undantag för punkt 1 g, h och i*** i denna artikel, anses vara uppfylld genom att reglerna om interna styrelseformer, arrangemang ***eller processer*** efterlevs enligt ***relevant unionsrätt om finansiella tjänster***. I detta syfte ska alla harmoniserade standarder som avses i artikel 40 beaktas.

Artikel 18

Bevarande av dokumentation

1. ***Leverantören ska under en period på 10 år efter det att AI-systemet med hög risk har släppts ut på marknaden eller tagits i bruk, för de nationella behöriga myndigheternas räkning hålla tillgängligt***

   a) den tekniska dokumentation som avses i punkt 11,

   b) den dokumentation avseende kvalitetsstyrningssystemet som det hänvisas till i artikel 17,

   c) i tillämpliga fall, dokumentation om de ändringar som godkänts av anmälda organ,

   d) i tillämpliga fall, de beslut och andra handlingar som utfärdats av de anmälda organen,

   e) EU-försäkran om överensstämmelse enligt artikel 47.

2. ***Varje medlemsstat ska fastställa på vilka villkor den dokumentation som avses i punkt 1 ska hållas tillgänglig för de nationella behöriga myndigheterna under den period som anges i den punkten i de fall då en leverantör eller dennes ombud som är etablerad på dess territorium går i konkurs eller upphör med sin verksamhet före utgången av denna period.***

3. Leverantörer som är ***finans***institut ***som omfattas av krav avseende sina interna styrelseformer, arrangemang eller processer enligt unionsrätten om finansiella tjänster*** ska bevara den tekniska dokumentationen som en del av den dokumentation ***som ska bevaras enligt relevant unionsrätt om finansiella tjänster***.

I

Artikel 19

Automatiskt genererade loggar

1. Leverantörer av AI-system med hög risk ska spara de loggar ***enligt artikel 12.1*** som genereras automatiskt av deras AI-system med hög risk, i den mån sådana loggar står under deras kontroll. ***Utan att det påverkar tillämplig unionsrätt eller nationell rätt*** ska loggarna sparas under en period ▌ som är lämplig ***för*** det avsedda ändamålet med AI-systemet med hög risk ***eller i minst sex månader, om inte annat föreskrivs i tillämplig*** unionsrätt eller nationell rätt***, i synnerhet unionsrätten om skydd av personuppgifter***.

2. Leverantörer som är ***finans***institut ***som omfattas av krav avseende sina interna styrelseformer, arrangemang eller processer enligt unionsrätten om finansiella tjänster*** ska bevara de loggar som genereras automatiskt av deras AI-system med hög risk som en del av den dokumentation ***som ska bevaras*** enligt ***relevant rätt om finansiella tjänster***.

Artikel 20

Korrigerande åtgärder ***och informationsplikt***

1. Leverantörer av AI-system med hög risk som anser eller har skäl att tro att ett AI-system med hög risk som de har släppt ut på marknaden eller tagit i bruk inte överensstämmer med denna förordning ska omedelbart vidta de korrigerande åtgärder som krävs för att, beroende på vad som är lämpligt, få systemet att överensstämma med kraven, dra tillbaka det***, inaktivera det*** eller återkalla det. De ska underrätta distributörerna av det berörda AI-systemet med hög risk och, i förekommande fall, ***spridarna,*** ombudet och importörerna om detta.

2. ***Om AI-systemet med hög risk utgör en risk i den mening som avses i artikel 79.1 och leverantören blir medveten om denna risk, ska den omedelbart utreda orsakerna, i samarbete med den rapporterande spridaren, i tillämpliga fall, och informera marknadskontrollmyndigheterna i den eller de medlemsstater där den har tillhandahållit AI-systemet med hög risk på marknaden och, i tillämpliga fall, det anmälda organ som utfärdat ett intyg för detta AI-system med hög risk i enlighet med artikel 44, särskilt om typen av bristande överensstämmelse och om eventuella relevanta korrigerande åtgärder som vidtagits.***

▌

Artikel 21

Samarbete med behöriga myndigheter

1. Leverantörer av AI-system med hög risk ska på ***motiverad*** begäran av en ▌ behörig myndighet förse den myndigheten med ▌ all information och dokumentation som krävs för att visa att AI-systemet med hög risk överensstämmer med kraven i avsnitt 2, på ***ett*** språk ***som är lätt att förstå*** för ***myndigheten och som är ett av unionsinstitutionernas officiella språk som anges av den berörda medlemsstaten***.

2. ***På motiverad begäran av en nationell behörig myndighet ska leverantörer också ge den begärande nationella behöriga myndigheten, i tillämpliga fall, tillgång till de automatiskt genererade loggar för AI-systemet med hög risk som avses i artikel 12.1, i den mån sådana loggar står under deras kontroll.***

3. All information som har erhållits av en nationell behörig myndighet i enlighet med denna artikel ska behandlas i enlighet med de konfidentialitetskrav som anges i artikel 78.

Artikel 22

Ombud för leverantörer av AI-system med hög risk

1. Innan leverantörer etablerade i tredjeländer tillhandahåller sina AI-system med hög risk på unionsmarknaden ▌ ska de genom skriftlig fullmakt utse ett ombud som är etablerat i unionen.

2. Leverantören ska göra det möjligt för sitt ombud att utföra de uppgifter som anges i fullmakten från leverantören.

3. Ombudet ska utföra de uppgifter som anges i fullmakten från leverantören. ***Ombudet ska på begäran lämna en kopia av fullmakten till marknadskontrollmyndigheterna på ett av unionsinstitutionernas officiella språk som anges av den nationella behöriga myndigheten. Vid tillämpning av denna förordning*** ska fullmakten ge ombudet befogenhet att utföra följande uppgifter:

a) Kontrollera att EU-försäkran om överensstämmelse och den tekniska dokumentation som avses i artikel 11 har upprättats och att leverantören har utfört ett lämpligt förfarande för bedömning av överensstämmelse.

b) ***Under en period på tio år efter det att AI-systemet med hög risk har släppts ut på marknaden eller tagits i bruk*** hålla ***kontaktuppgifterna*** till den ***leverantör som utsåg ombudet, en kopia av EU-försäkran om överensstämmelse, den tekniska dokumentationen och, i tillämpliga fall, det intyg som utfärdats av det anmälda organet tillgängliga*** för de ***nationella behöriga myndigheter och nationella myndigheter eller organ som avses i artikel 74.10***.

c) På motiverad begäran ge en nationell behörig myndighet all information och dokumentation***, inbegripet den som avses i led b i detta stycke,*** som är nödvändig för att visa att ett AI-system med hög risk överensstämmer med kraven i avsnitt 2, inbegripet tillgång till de loggar ***enligt artikel 12.1*** som automatiskt genereras av AI-systemet med hög risk, i den mån sådana loggar står under leverantörens kontroll ▌ .

d) På motiverad begäran samarbeta med behöriga ▌ myndigheter i eventuella åtgärder som dessa vidtar med avseende på AI-systemet med hög risk, ***i synnerhet för att minska och begränsa de risker som AI-systemet med hög risk utgör***.

e) I tillämpliga fall, fullgöra de registreringsskyldigheter som avses i artikel 49.1 eller, om registreringen utförs av leverantören själv, säkerställa att den information som avses i avsnitt A i ***bilaga VIII är korrekt.***

Fullmakten ska ge ombudet befogenhet att utöver eller i stället för leverantören stå till förfogande inför de behöriga myndigheterna, i alla frågor som rör efterlevnaden av denna förordning.

4. Ombudet ska säga upp fullmakten om denne anser eller har skäl att tro att leverantören agerar i strid med sina skyldigheter enligt denna förordning. I sådana fall ska det också omedelbart underrätta marknadskontrollmyndigheten i den medlemsstat där det befinner sig eller är etablerat samt, i tillämpliga fall, det berörda anmälda organet om uppsägningen av fullmakten och skälen till detta.

Artikel 23

Importörers skyldigheter

1. Innan importörer släpper ut ett AI-system med hög risk på marknaden ska de säkerställa att ***systemet överensstämmer med denna förordning genom att kontrollera att***

a) det ***tillämpliga*** förfarandet för bedömning av överensstämmelse ***enligt artikel 43*** har utförts av leverantören av AI-systemet med hög risk,

b) leverantören har upprättat den tekniska dokumentationen i enlighet med ***artikel 11 och*** bilaga IV,

c) systemet är försett med erforderlig ***CE***-märkning och åtföljs av ***EU-försäkran om överensstämmelse*** och bruksanvisning***,***

d) leverantören har utsett ett ombud i enlighet med artikel 22.1.

2. Om en importör ***har tillräckliga*** skäl att tro att ett AI-system med hög risk inte överensstämmer med denna förordning, ***är förfalskat eller åtföljs av förfalskad dokumentation*** ska den inte släppa ut systemet på marknaden förrän det har bringats i överensstämmelse med kraven. Om AI-systemet med hög risk utgör en risk i den mening som avses i artikel 79.1 ska importören informera leverantören av systemet***, ombuden*** och marknadskontrollmyndigheterna om detta.

3. Importörer ska ange sitt namn, sitt registrerade firmanamn eller sitt registrerade varumärke och en kontaktadress avseende AI-systemet med hög risk på dess förpackning eller i dess åtföljande dokumentation, ***i*** tillämpliga ***fall***.

4. Importörer ska så länge de har ansvar för ett AI-system med hög risk säkerställa att lagrings- eller transportförhållanden, i förekommande fall, inte äventyrar dess överensstämmelse med kraven i avsnitt 2.

5. ***Importörer ska under en period på tio år efter det att AI-systemet med hög risk har släppts ut på marknaden eller tagits i bruk bevara en kopia av det intyg som utfärdats av det anmälda organet, i tillämpliga fall, av bruksanvisningen och av EU-försäkran om överensstämmelse.***

6. Importörer ska på motiverad begäran ge nationella behöriga myndigheter all information och dokumentation som är nödvändig, ***inbegripet den som förvaras i enlighet med punkt 5,*** för att visa att ett AI-system med hög risk överensstämmer med kraven i avsnitt 2 på ett språk som lätt kan förstås av ***dem. I detta syfte*** ska de också ***säkerställa att den tekniska dokumentationen kan göras tillgänglig för dessa myndigheter***.

7. ***Importörerna ska samarbeta med de nationella behöriga myndigheterna i alla åtgärder som dessa myndigheter vidtar med avseende på ett AI-system med hög risk som importörerna har släppt ut på marknaden, i synnerhet för att minska och begränsa de risker som det utgör.***

Artikel 24

Distributörers skyldigheter

1. Innan distributörer tillhandahåller ett AI-system med hög risk på marknaden ska de kontrollera att det är försett med erforderlig CE-märkning, att det åtföljs av ***en kopia av EU-försäkran om överensstämmelse*** och bruksanvisningen och att leverantören och importören av systemet, beroende på vad som är tillämpligt, har uppfyllt ***sina*** respektive skyldigheter enligt ***artiklarna 16 b och c samt 23.3***.

2. Om en distributör ***– på grundval av den information som denne har kännedom om –*** anser eller har skäl att tro att ett AI-system med hög risk inte överensstämmer med kraven i avsnitt 2, får distributören inte tillhandahålla AI-systemet med hög risk på marknaden förrän systemet har bringats i överensstämmelse med dessa krav. Om AI-systemet med hög risk utgör en risk i den mening som avses i artikel 79.1 ska distributören dessutom informera leverantören eller importören av systemet, beroende på vad som är tillämpligt, om detta.

3. Distributörer ska så länge de har ansvar för ett AI-system med hög risk säkerställa att, i förekommande fall, lagrings- eller transportförhållanden inte äventyrar systemets överensstämmelse med kraven i avsnitt 2.

4. En distributör som ***– på grundval av den information som denne har kännedom om –*** anser eller har skäl att tro att ett AI-system med hög risk som denne har tillhandahållit på marknaden inte överensstämmer med kraven i avsnitt 2 ska vidta de korrigerande åtgärder som krävs för att bringa systemet i överensstämmelse med dessa krav, dra tillbaka det eller återkalla det, eller ska säkerställa att leverantören, importören eller någon berörd operatör, beroende på vad som är lämpligt, vidtar dessa korrigerande åtgärder. Om AI-systemet med hög risk utgör en risk i den mening som avses i artikel 79.1 ska distributören omedelbart informera ***leverantören eller importören av systemet och de*** nationella behöriga myndigheterna i de medlemsstater där distributören har tillhandahållit produkten om detta och lämna uppgifter särskilt om den bristande överensstämmelsen och om eventuella korrigerande åtgärder som vidtagits.

5. På motiverad begäran av en nationell behörig myndighet ska distributörer av ***ett AI-system med hög risk*** förse den myndigheten med all information och dokumentation ***om deras åtgärder enligt punkterna 1–4*** som är nödvändig för att visa att det systemet uppfyller kraven i avsnitt 2. ▌

6. Distributörerna ska samarbeta med de nationella behöriga myndigheterna i alla åtgärder som dessa myndigheter vidtar med avseende på ett AI-system med hög risk som de har gjort tillgängligt på marknaden, i synnerhet för att minska eller begränsa den risk som det utgör.

Artikel 25

Ansvar längs AI-värdekedjan

1. Varje distributör, importör, ***spridare*** eller annan tredje part ska vid tillämpningen av denna förordning anses vara en leverantör ***av ett AI-system med hög risk*** och ha de skyldigheter som leverantören har enligt artikel 16, under någon av följande omständigheter:

   a) De ***sätter sitt namn eller varumärke på ett AI-system med hög risk som redan släppts ut*** på marknaden eller tagits i bruk***, utan att det påverkar avtalsarrangemang som föreskriver att skyldigheterna däri ska fördelas på annat sätt.***

   b) De ***gör en väsentlig ändring av*** ett AI-system med hög risk ***som*** redan ***har*** släppts ut på marknaden eller ***redan har*** tagits i bruk ***på ett sådant sätt att det fortfarande är ett AI-system med hög risk enligt artikel 6***.

c) De ändrar det avsedda ändamålet för ett AI-system, inklusive ett AI-system för allmänna ändamål, som inte har klassificerats som ett högrisksystem och som redan har släpps ut på marknaden eller tagits i bruk på ett sådant sätt att det berörda AI-systemet blir ett AI-system med hög risk i enlighet med artikel 6.

▌

2. Om de omständigheter som avses i punkt 1 uppstår, ska den leverantör som ursprungligen släppte ut AI-systemet ▌ på marknaden eller tog det i bruk inte längre anses vara en leverantör ***av det specifika AI-systemet*** vid tillämpningen av denna förordning. ***Den ursprungliga leverantören ska nära samarbeta med nya leverantörer och tillgängliggöra den nödvändiga informationen och tillhandahålla den rimligen förväntade tekniska åtkomsten och annat stöd som krävs för att fullgöra de skyldigheter som fastställs i denna förordning, särskilt när det gäller efterlevnaden av bedömningen av överensstämmelse för AI-system med hög risk. Denna punkt ska inte tillämpas i fall där den ursprungliga leverantören tydligt har angett att dess AI-system inte får omvandlas till ett AI-system med hög risk och därför inte omfattas av skyldigheten att överlämna dokumentationen.***

3. ***När det gäller AI-system med hög risk som är säkerhetskomponenter i produkter*** som omfattas av den unionslagstiftning om harmonisering ***som förtecknas i avsnitt A i bilaga I, ska produkttillverkaren anses vara leverantören av AI-systemet med hög risk och omfattas av de skyldigheter som avses i artikel 16 under någon av följande omständigheter:***

a) ***AI-systemet med hög risk släpps ut på marknaden tillsammans med produkten under produkttillverkarens namn eller varumärke.***

b) ***AI-systemet med hög risk tas i bruk under produkttillverkarens namn eller varumärke efter det att produkten släppts ut på marknaden.***

4. ***Leverantören av ett AI-system med hög risk och den tredje part som tillhandahåller ett AI-system, verktyg, tjänster, komponenter eller processer som används eller integreras i ett AI-system med hög risk ska genom ett skriftligt avtal ange den nödvändiga informationen, kapaciteten och tekniska åtkomsten samt det andra stödet, baserat på teknikens allmänt erkända ståndpunkt, för att göra det möjligt för leverantören av AI-systemet med hög risk att fullt ut uppfylla de skyldigheter som fastställs i denna förordning. Denna punkt ska inte tillämpas på tredje parter som genom en fri och öppen licens för allmänheten tillgängliggör andra verktyg, tjänster, processer eller komponenter än AI-modeller för allmänna ändamål.***

AI-byrån får utveckla och rekommendera frivilliga standardvillkor för avtal mellan leverantörer av AI-system med hög risk och tredje parter som tillhandahåller verktyg, tjänster, komponenter eller processer som används för eller är integrerade i AI-system med hög risk. Vid utarbetandet av dessa frivilliga standardvillkor ska AI-byrån ta hänsyn till eventuella avtalskrav som är tillämpliga inom specifika sektorer eller affärsfall. De frivilliga standardvillkoren ska offentliggöras och vara tillgängliga kostnadsfritt i ett lättanvänt elektroniskt format.

5. ***Punkterna 2 och 3 ska inte påverka behovet av att iaktta och skydda immateriella rättigheter, konfidentiell affärsinformation och företagshemligheter i enlighet med unionsrätten och nationell rätt.***

Artikel 26

Skyldigheter för ***spridare*** *av AI-system med hög risk*

1. ***Spridare*** av AI-system med hög risk ska ***vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att de*** använder sådana system i enlighet med de bruksanvisningar som åtföljer systemen, enligt punkterna 3 och 6.

2. ***Spridarna ska tilldela fysiska personer som har nödvändig kompetens, utbildning och auktoritet samt nödvändigt stöd uppgiften att utöva mänsklig tillsyn.***

3. De skyldigheter som fastställs i punkterna 1 ***och 2*** ska inte påverka andra ***spridar***skyldigheter enligt unionsrätten eller nationell rätt eller ***spridarens*** frihet att organisera sina egna resurser och sin egen verksamhet i syfte att genomföra de åtgärder för mänsklig tillsyn som leverantören anger.

4. Utan att det påverkar tillämpningen av punkterna 1 ***och 2*** ska ***spridaren***, i den mån ***spridaren*** utövar kontroll över indata, säkerställa att indata är relevanta ***och tillräckligt representativa*** med tanke på det avsedda ändamålet med AI-systemet med hög risk.

5. ***Spridarna*** ska övervaka driften av AI-systemet med hög risk på grundval av bruksanvisningen ***och, i förekommande fall, informera leverantörerna i enlighet med artikel 72***. Om spridarna har skäl att tro att användningen av AI-systemet med hög risk i enlighet med instruktionerna kan utgöra en risk i den mening som avses i artikel 79.1 ska de***, utan onödigt dröjsmål,*** informera leverantören eller distributören och den ***berörda marknadskontrollmyndigheten och*** tillfälligt avbryta användningen av det systemet. Om spridare har fastställt en allvarlig incident ska de också ***omedelbart*** informera ***först*** leverantören ***och sedan importören*** eller distributören ***och de berörda marknadskontrollsmyndigheterna*** om den incidenten. ***Om spridaren inte kan nå leverantören ska artikel 73 gälla i tillämpliga delar. Denna skyldighet ska inte omfatta känsliga operativa uppgifter om spridare av AI-system som är brottsbekämpande myndigheter***.

För ***spridare*** som är ***finans***institut ***som omfattas av krav avseende sina interna styrelseformer, arrangemang eller processer enligt unionsrätten om finansiella tjänster*** ska övervakningsskyldigheten i första stycket anses vara uppfylld genom att reglerna om interna styrelseformer, arrangemang, processer och mekanismer enligt ***relevant unionsrätt om finansiella tjänster*** följs.

6. ***Spridare*** av AI-system med hög risk ska spara de loggar som genereras automatiskt av det AI-systemet med hög risk, ▌ i den mån sådana loggar står under deras kontroll, ▌ under en period ▌ som är lämplig ***för*** det avsedda ändamålet med AI-systemet med hög risk***, dock i minst sex månader, om inte annat föreskrivs i tillämplig*** unionsrätt eller nationell rätt***, i synnerhet unionsrätten om skydd av personuppgifter***.

Spridare som är ***finans***institut ***som omfattas av krav avseende sina interna styrelseformer, arrangemang eller processer enligt unionsrätten om finansiella tjänster*** ska bevara loggar som en del av den dokumentation ***som ska bevaras*** enligt ***relevant unionsrätt om finansiella tjänster***.

7. Innan ett AI-system med hög risk tas i bruk eller används på arbetsplatsen ska spridare som är arbetsgivare informera arbetstagarrepresentanterna och de berörda arbetstagarna om att de kommer att vara föremål för användning av AI-systemet med hög risk. Denna information ska, i tillämpliga fall, tillhandahållas i enlighet med de regler och förfaranden som fastställs i unionsrätten och nationell rätt samt praxis i fråga om information till arbetstagare och deras representanter.

8. Spridare av AI-system med hög risk som är offentliga myndigheter eller unionens institutioner, organ eller byråer ska fullgöra de registreringsskyldigheter som avses i artikel 49. Om dessa spridare finner att det AI-system med hög risk som de avser att använda inte har registrerats i den EU-databas som avses i artikel 71 ska de inte använda det systemet utan informera leverantören eller distributören.

9. ***I tillämpliga fall*** ska ***spridare*** av AI-system med hög risk använda den information som tillhandahålls enligt artikel 13 i denna förordning för att fullgöra sin skyldighet att genomföra en konsekvensbedömning avseende dataskydd enligt artikel 35 i förordning (EU) 2016/679 eller artikel 27 i direktiv (EU) 2016/680. ▌

10. Inom ramen för en utredning för målinriktad sökning av en person som misstänks ha begått ett brott eller som har dömts för att ha begått ett brott ska spridaren av ett AI-system med hög risk ***för biometrisk fjärridentifiering i efterhand, utan att det påverkar tillämpningen av direktiv (EU) 2016/680, på förhand eller utan onödigt dröjsmål och senast inom 48 timmar, av en rättslig myndighet eller en administrativ myndighet vars beslut är bindande och föremål för rättslig prövning begära tillstånd för användning av det systemet, utom när det används för den inledande identifieringen av en potentiell misstänkt på grundval av objektiva och verifierbara fakta med direkt anknytning till brottet. Varje användning ska begränsas till vad som är absolut nödvändigt för att utreda ett specifikt brott.***

Om det begärda tillstånd som föreskrivs i första stycket avslås ska användningen av det system för biometrisk fjärridentifiering i efterhand som är kopplat till det begärda tillståndet upphöra med omedelbar verkan, och de personuppgifter som är kopplade till användningen av det AI-system med hög risk ***för vilket tillståndet begärdes ska raderas.***

Under inga omständigheter får ett sådant AI-system med hög risk ***för biometrisk fjärridentifiering i efterhand användas för brottsbekämpningsändamål på ett icke målinriktat sätt, utan koppling till ett brott, ett straffrättsligt förfarande, ett verkligt och aktuellt eller verkligt och förutsebart hot om ett brott eller sökning efter en specifik försvunnen person. Det ska säkerställas att inget beslut som har negativa rättsliga följder för en person får fattas av de brottsbekämpande myndigheterna enbart på grundval av utdata från sådana system för biometrisk fjärridentifiering i efterhand.***

Denna punkt påverkar inte tillämpningen av artikel 9 i förordning (EU) 2016/679 och artikel 10 i direktiv (EU) 2016/680 avseende behandling av biometriska uppgifter.

Oavsett ändamål eller spridare ska varje användning av sådana AI-system med hög risk ***dokumenteras i den relevanta polisakten och på begäran göras tillgänglig för den berörda marknadskontrollmyndigheten och den nationella dataskyddsmyndigheten, med undantag för utlämnande av känsliga operativa uppgifter som rör brottsbekämpning. Detta stycke ska inte påverka de befogenheter som tilldelas tillsynsmyndigheterna genom direktiv (EU) 2016/680.***

Spridarna ska lämna in årliga rapporter till de berörda marknadskontrollmyndigheterna och nationella dataskyddsmyndigheterna om sin användning av system för biometrisk fjärridentifiering i efterhand, med undantag för utlämnande av känsliga operativa uppgifter som rör brottsbekämpning. Rapporterna får aggregeras för att täcka mer än en användning.

Medlemsstaterna får införa mer restriktiva lagar om användningen av system för biometrisk fjärridentifiering i efterhand i enlighet med unionsrätten.

11. Utan att det påverkar tillämpningen av artikel 50 i denna förordning ska spridare av AI-system med hög risk som avses i bilaga III och som fattar beslut eller hjälper till att fatta beslut som rör fysiska personer informera de fysiska personerna om att de är föremål för användning av AI-systemet med hög risk. När det gäller AI-system med hög risk som används för brottsbekämpningsändamål ska artikel 13 i direktiv (EU) 2016/680 tillämpas.

12. Spridarna ska samarbeta med de berörda nationella behöriga myndigheterna i alla åtgärder som dessa myndigheter vidtar med avseende på AI-systemet med hög risk i syfte att genomföra denna förordning.

Artikel 27

Konsekvensbedömning avseende grundläggande rättigheter när det gäller AI-system med hög risk

1. Innan ett AI-system med hög risk som avses i artikel 6.2 börjar användas, med undantag för AI-system med hög risk som är avsedda att användas inom det område som anges i punkt 2 i bilaga III, ska spridare som är offentligrättsliga organ eller som är privata enheter som tillhandahåller offentliga tjänster, och spridare av AI-system med hög risk som avses i punkt 5 b** och c i bilaga ***III, göra en bedömning av den inverkan på de grundläggande rättigheterna som användningen av ett sådant system kan ge upphov till. För detta ändamål ska spridarna göra en bedömning bestående av följande:

a) En beskrivning av spridarens processer där AI-systemet med hög risk kommer att användas i linje med dess avsedda ändamål.

b) En beskrivning av den tidsperiod inom vilken och den frekvens med vilken varje AI-system med hög risk är avsett att användas.

c) De kategorier av fysiska personer och grupper som sannolikt kommer att påverkas av användningen av systemet i det specifika sammanhanget.

d) De specifika risker för skada som sannolikt kommer att påverka de kategorier av personer eller grupper av personer som har identifierats i enlighet med led c i denna punkt, med beaktande av den information som leverantören har tillhandahållit i enlighet med artikel 13.

e) En beskrivning av genomförandet av åtgärder för mänsklig tillsyn, i enlighet med bruksanvisningen.

f) De åtgärder som ska vidtas när dessa risker förverkligas, inbegripet arrangemangen för intern styrning och klagomålsmekanismer.

2. Den skyldighet som fastställs i punkt 1 gäller för den första användningen av AI-systemet med hög risk. Spridaren får i liknande fall förlita sig på tidigare genomförda konsekvensbedömningar avseende grundläggande rättigheter eller befintliga konsekvensbedömningar som har utförts av leverantören. En spridare som under användningen av AI-systemet med hög risk anser att något av de element som anges i punkt 1 har ändrats eller inte längre är aktuellt ska vidta nödvändiga åtgärder för att uppdatera informationen.

3. När den bedömning som avses i punkt 1 i denna artikel har utförts ska spridaren underrätta marknadskontrollmyndigheten om sina resultat, inbegripet fylla i och lämna in den mall som avses i punkt 5 i denna artikel som en del av underrättelsen. I det fall som avses i artikel 46.1 får spridare undantas från den underrättelseskyldigheten.

4. Om någon av de skyldigheter som fastställs i denna artikel redan uppfylls till följd av den konsekvensbedömning avseende dataskydd som genomförs i enlighet med artikel 35 i förordning (EU) 2016/679 eller artikel 27 i direktiv (EU) 2016/680, ska den konsekvensbedömning avseende grundläggande rättigheter som avses i punkt 1 i denna artikel komplettera den konsekvensbedömningen avseende dataskydd.

5. AI-byrån ska utarbeta en mall för ett frågeformulär, inbegripet genom ett automatiserat verktyg, för att underlätta för spridarna att på ett förenklat sätt fullgöra sina skyldigheter enligt denna artikel.

Avsnitt 4

Anmälande myndigheter och anmälda organ

Artikel 28

Anmälande myndigheter

1. Varje medlemsstat ska utse eller inrätta ***minst en*** anmälande myndighet med ansvar för att fastställa och genomföra de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och för övervakning av dessa. ***Dessa förfaranden ska utvecklas i samarbete mellan de anmälande myndigheterna i alla medlemsstater.***

2. Medlemsstaterna får ***bestämma att den bedömning och övervakning som avses i punkt 1 ska utföras av*** ett nationellt ackrediteringsorgan ***i den mening som avses i, och i enlighet med,*** förordning (EG) nr 765/2008 .

3. Anmälande myndigheter ska vara inrättade och organiserade och fungera på ett sådant sätt att det inte uppstår någon intressekonflikt med organen för bedömning av överensstämmelse och att det garanteras att deras verksamhet är objektiv och opartisk.

4. Anmälande myndigheter ska vara organiserade på ett sådant sätt att beslut som rör anmälan av organ för bedömning av överensstämmelse fattas av annan behörig personal än den som har gjort bedömningen av dessa organ.

5. Anmälande myndigheter får varken erbjuda eller utföra sådan verksamhet som utförs av organ för bedömning av överensstämmelse eller erbjuda eller utföra konsulttjänster på kommersiell eller konkurrensmässig grund.

6. Anmälande myndigheter ska säkerställa att den information som de erhåller behandlas konfidentiellt, ***i enlighet med artikel 78***.

7. Anmälande myndigheter ska förfoga över ***tillräckligt*** med personal med lämplig kompetens för att kunna utföra sina uppgifter. ***Kompetent personal ska, i tillämpliga fall, ha nödvändig sakkunskap med tanke på sin funktion, på områden som informationsteknik, AI och juridik, inbegripet övervakning av de grundläggande rättigheterna.***

Artikel 29

Ansökan om anmälan från ett organ för bedömning av överensstämmelse

1. Organ för bedömning av överensstämmelse ska lämna in en ansökan om anmälan till den anmälande myndigheten i den medlemsstat där de är etablerade.

2. Ansökan om anmälan ska åtföljas av en beskrivning av de bedömningar av överensstämmelse, den eller de moduler för bedömning av överensstämmelse och de ***typer av AI-system*** som organet för bedömning av överensstämmelse anser sig ha kompetens för samt ett ackrediteringsintyg, om sådant finns, som ska ha utfärdats av ett nationellt ackrediteringsorgan och i vilket det intygas att organet för bedömning av överensstämmelse uppfyller kraven i artikel 31.

   Alla giltiga dokument som rör fall av befintligt utseende av det ansökande anmälda organet enligt annan unionslagstiftning om harmonisering ska läggas till.

3. Om det berörda organet för bedömning av överensstämmelse inte kan uppvisa något ackrediteringsintyg ska det ge den anmälande myndigheten ***alla*** skriftliga underlag som krävs för kontroll, erkännande och regelbunden övervakning av att det uppfyller kraven i artikel 31.

4. För anmälda organ som utsetts enligt annan unionslagstiftning om harmonisering får alla dokument och intyg kopplade till dessa fall av utseende användas som stöd för deras utseendeförfarande enligt denna förordning, beroende på vad som är lämpligt. ***Det anmälda organet ska uppdatera den dokumentation som avses i punkterna 2 och 3 i denna artikel när det sker relevanta ändringar, för att myndigheten med ansvar för anmälda organ ska kunna övervaka och kontrollera att samtliga krav som föreskrivs i artikel 31 alltid uppfylls.***

Artikel 30

Anmälningsförfarande

1. De anmälande myndigheterna får ▌ endast ***anmäla*** de organ för bedömning av överensstämmelse som uppfyller kraven i artikel 31.

2. De anmälande myndigheterna ska till kommissionen och övriga medlemsstater, med hjälp av det elektroniska anmälningsverktyg som har utvecklats och förvaltas av kommissionen, anmäla ***varje organ för bedömning av överensstämmelse som avses i punkt 1***.

3. Den anmälan ***som avses i punkt 2 i denna artikel*** ska innehålla fullständiga uppgifter om bedömningarna av överensstämmelse, modulen eller modulerna för bedömning av överensstämmelse, de berörda ***typerna av AI-system samt ett relevant intyg om kompetens***. ***Om en anmälan inte grundar sig på ett sådant ackrediteringsintyg som avses i artikel 29.2 ska den anmälande myndigheten ge kommissionen och övriga medlemsstater styrkande handlingar som visar att organet för bedömning av överensstämmelse har erforderlig kompetens och att de system har inrättats som behövs för att säkerställa att organet övervakas regelbundet och fortsätter att uppfylla kraven i artikel 31***.

4. Det berörda organet för bedömning av överensstämmelse får bedriva verksamhet som anmält organ endast om kommissionen och övriga medlemsstater inte har gjort några invändningar inom ***två veckor från en anmälan från en anmälande myndighet, i de fall ett ackrediteringsintyg enligt artikel 29.2 används, eller inom två månader*** från anmälan ***från den anmälande myndigheten, i de fall då styrkande handlingar som avses i artikel 29.3 används***.

5. Om invändningar görs ska kommissionen utan dröjsmål inleda samråd med de berörda medlemsstaterna och organet för bedömning av överensstämmelse. Med beaktande av detta ska kommissionen besluta om tillståndet är motiverat eller inte. Kommissionen ska rikta sitt beslut till medlemsstaten i fråga och det berörda organet för bedömning av överensstämmelse.

Artikel 31

Krav avseende anmälda organ

1. ***Ett*** anmält ***organ*** ska ***inrättas i enlighet med en medlemsstats nationella rätt och ska vara en juridisk person***.

2. Anmälda organ ska uppfylla de organisatoriska krav och krav på kvalitetsstyrning, resurser och processer som är nödvändiga för att de ska kunna fullgöra sina uppgifter***, samt lämpliga cybersäkerhetskrav***.

3. Det anmälda organets organisationsstruktur, ansvarsfördelning, rapporteringsvägar och driftsätt ska säkerställa förtroende för dess prestationer och för resultaten av de aktiviteter avseende bedömning av överensstämmelse som det anmälda organet bedriver.

4. Anmälda organ ska vara oberoende av den leverantör av AI-system med hög risk som är föremål för dess bedömning av överensstämmelse. Anmälda organ ska också vara oberoende av varje annan operatör som har ett ekonomiskt intresse i AI-system med hög risk som bedöms samt av eventuella konkurrenter till leverantören. ***Detta ska inte hindra att bedömda AI-system med hög risk som är nödvändiga för verksamheten inom organet för bedömning av överensstämmelse används, eller att sådana AI-system med hög risk används för personligt bruk.***

5. Varken ***ett organ för bedömning av överensstämmelse, dess högsta ledning eller den personal som ansvarar för att utföra bedömningen av överensstämmelse får vara direkt inblandad i konstruktionen, utvecklingen, saluföringen eller användningen av AI-system med hög risk, och de får inte heller företräda de parter som bedriver sådan verksamhet. De får inte delta i någon verksamhet som kan påverka deras objektivitet eller integritet i samband med den bedömning av överensstämmelse för vilken de har anmälts. Detta ska framför allt gälla konsulttjänster.***

6. Anmälda organ ska vara organiserade och drivas på ett sådant sätt att deras verksamhet är oberoende, objektiv och opartisk. Anmälda organ ska dokumentera och genomföra en struktur och förfaranden som garanterar opartiskheten och främjar och tillämpar principerna om opartiskhet i hela organisationen, hos alla anställda och i all bedömningsverksamhet.

7. Anmälda organ ska ha infört dokumenterade förfaranden som ska säkerställa att deras personal, kommittéer, dotterbolag, underentreprenörer och andra associerade organ eller personal vid externa organ ***i enlighet med artikel 78*** upprätthåller konfidentialiteten för den information som organen får kännedom om i samband med bedömning av överensstämmelse, utom när informationen måste lämnas ut enligt lag. De anmälda organens personal ska vara ålagd tystnadsplikt i fråga om all information som de erhåller under utförandet av sina uppgifter enligt denna förordning, utom gentemot de anmälande myndigheterna i den medlemsstat där deras verksamhet utförs.

8. Anmälda organ ska ha förfaranden som gör det möjligt för organet att utöva sin verksamhet med vederbörlig hänsyn tagen till en leverantörs storlek, sektor och struktur samt det berörda AI-systemets komplexitet.

9. Anmälda organ ska teckna en lämplig ansvarsförsäkring för sin verksamhet avseende bedömningar av överensstämmelse, såvida inte den medlemsstat ***i vilken de är etablerade*** tar på sig ansvaret i överensstämmelse med nationell rätt eller den medlemsstaten är direkt ansvarig för bedömningen av överensstämmelse.

10. Anmälda organ ska kunna utföra alla sina uppgifter enligt denna förordning med högsta yrkesmässiga integritet och nödvändig kompetens på det specifika området, oavsett om dessa uppgifter utförs av de anmälda organen själva eller av annan part för deras räkning och under deras ansvar.

11. Anmälda organ ska ha tillräcklig intern kompetens för att effektivt kunna utvärdera de uppgifter som utförs av externa parter å organens vägnar. ▌ Det anmälda organet ska ständigt ha tillräcklig administrativ, teknisk, ***juridisk*** och vetenskaplig personal med erfarenhet av och kunskaper om de relevanta ***typerna av*** AI-***system***, relevanta data och relevant databehandling och om de krav som fastställs i avsnitt 2.

12. Anmälda organ ska delta i den samordningsverksamhet som avses i artikel 38. De ska också delta direkt, eller vara företrädda i, europeiska standardiseringsorganisationer, eller säkerställa att de är medvetna om och har aktuella kunskaper om relevanta standarder.

Artikel 32

Presumtion om överensstämmelse med krav som rör anmälda organ

För ett organ för bedömning av överensstämmelse som kan visa att det uppfyller kriterierna i de relevanta harmoniserade standarderna eller delar av dem, till vilka hänvisningar har offentliggjorts i Europeiska unionens officiella tidning, ska en presumtion om överensstämmelse med kraven i artikel 31 gälla, på villkor att dessa krav omfattas av de tillämpliga harmoniserade standarderna.

Artikel 33

Dotterbolag till anmälda organ och underentreprenad

1. Om det anmälda organet lägger ut specifika uppgifter med anknytning till bedömningen av överensstämmelse på underentreprenad eller anlitar ett dotterbolag ska det säkerställa att underentreprenören eller dotterbolaget uppfyller kraven i artikel 31 och informera den anmälande myndigheten om detta.

2. De anmälda organen ska ta det fulla ansvaret för sina uppgifter som utförs av underentreprenörer eller dotterbolag.

3. Verksamhet får läggas ut på underentreprenad eller utföras av ett dotterbolag endast om leverantören samtycker till det. ***Anmälda organ ska offentliggöra en förteckning över sina dotterbolag.***

4. De relevanta dokumenten rörande bedömningen av underentreprenörens eller dotterbolagets kvalifikationer och det arbete som dessa har utfört i enlighet med denna förordning ***ska hållas tillgängliga för den anmälande myndigheten under en period av fem år från och med dagen för avslutandet av underentreprenörsverksamheten***.

Artikel 34

De anmälda organens operativa skyldigheter

1. Anmälda organ ska kontrollera överensstämmelsen hos AI-system med hög risk i enlighet med de förfaranden för bedömning av överensstämmelse som föreskrivs i artikel 43.

2. Anmälda organ ska motverka uppkomsten av onödiga administrativa bördor för leverantörer när de utövar sin verksamhet och ta vederbörlig hänsyn till en leverantörs storlek, den sektor där denna är verksam, dess struktur samt komplexiteten i det berörda AI-systemet med hög risk, särskilt i syfte att minimera de administrativa bördorna och efterlevnadskostnaderna för mikroföretag och småföretag i den mening som avses i rekommendation 2003/361/EG. Det anmälda organet ska emellertid respektera den grad av noggrannhet och den skyddsnivå som krävs för att AI-systemet med hög risk ska överensstämma med kraven i denna förordning. .

3. Anmälda organ ska tillhandahålla och på begäran lämna över all relevant dokumentation, inbegripet leverantörens dokumentation, till den anmälande myndighet som avses i artikel 28, så att denna myndighet kan utföra sina uppgifter avseende bedömning, utseende, anmälan och övervakning och för att underlätta den bedömning som beskrivs i detta avsnitt.

Artikel 35

Identifikationsnummer och förteckningar över anmälda organ

1. Kommissionen ska tilldela varje anmält organ ett enda identifikationsnummer, även om ett organ anmäls i enlighet med mer än en unionsakt.

2. Kommissionen ska offentliggöra förteckningen över de organ som anmälts i enlighet med denna förordning, inklusive deras identifikationsnummer och den verksamhet som de har anmälts för. Kommissionen ska säkerställa att förteckningen hålls uppdaterad.

Artikel 36

Ändringar i anmälan

1. Den anmälande myndigheten ska underrätta kommissionen och övriga medlemsstater om alla relevanta ändringar beträffande anmälan av ett anmält organ via det elektroniska anmälningsverktyg som avses i artikel 30.2.

2. De förfaranden som föreskrivs i artiklarna 29 och 30 ska tillämpas på utvidgningar av anmälans tillämpningsområde.

När det gäller andra ändringar av anmälan än utvidgningar av dess tillämpningsområde ska de förfaranden som fastställs i följande punkter tillämpas.

3. ***Om ett anmält organ beslutar att upphöra med sin verksamhet avseende bedömning av överensstämmelse, ska det så snart som möjligt och, om upphörandet är planerat, minst ett år innan det upphör med verksamheten underrätta den anmälande myndigheten och de berörda leverantörerna om detta. Det anmälda organets intyg får förbli giltiga under en tillfällig period på nio månader efter det att det anmälda organets verksamhet upphört på villkor att ett annat anmält organ skriftligen har bekräftat att det kommer att ta ansvar för de AI-system med hög risk som omfattas av intygen. Det sistnämnda anmälda organet ska utföra en fullständig bedömning av de AI-system det gäller före utgången av denna niomånadersperiod, innan det utfärdar nya intyg för dem. Om det anmälda organet har upphört med sin verksamhet ska den anmälande myndigheten återkalla utseendet.***

4. Om en anmälande myndighet har ***tillräckliga skäl att anse*** att ett anmält organ inte längre uppfyller de krav som anges i artikel 31 eller att det underlåter att fullgöra sina skyldigheter, ska ***den anmälande*** myndigheten utan dröjsmål undersöka frågan med största möjliga omsorg. I detta sammanhang ska den anmälande myndigheten underrätta det berörda anmälda organet om de invändningar som framförts och ge det möjlighet att framföra sina synpunkter. Om en anmälande myndighet drar slutsatsen att ett anmält organ ▌ inte längre uppfyller de krav som anges i artikel 31 eller att det underlåter att fullgöra sina skyldigheter, ska den anmälande myndigheten, beroende på hur allvarlig underlåtenheten ***att uppfylla kraven eller fullgöra skyldigheterna*** är, begränsa utseendet, tillfälligt återkalla det eller återkalla det slutgiltigt ▌ beroende på vad som är lämpligt. Myndigheten ska ▌ omedelbart informera kommissionen och de andra medlemsstaterna om detta.

5. ***Om*** utseendet ***av ett anmält organ har återkallats tillfälligt eller begränsats, eller helt eller delvis återkallats slutgiltigt, ska det anmälda organet underrätta de berörda leverantörerna senast inom tio dagar***.

6. I händelse av begränsningar eller tillfällig eller slutgiltig återkallelse av ett utseende ska den anmälande myndigheten vidta lämpliga åtgärder för att säkerställa att det berörda anmälda organets dokumentation bevaras och göra den tillgänglig för de anmälande myndigheterna i andra medlemsstater och för marknadskontrollmyndigheterna på deras begäran.

7. I händelse av begränsningar eller tillfällig eller slutgiltig återkallelse av ett utseende ska den anmälande myndigheten

a) bedöma påverkan på de intyg som det anmälda organet har utfärdat,

b) överlämna en rapport om sina iakttagelser till kommissionen och de andra medlemsstaterna senast tre månader efter att ha anmält ändringarna av utseendet,

c) ålägga det anmälda organet att, inom en rimlig tid som myndigheten fastställer, tillfälligt eller slutgiltigt dra tillbaka intyg som utfärdats på felaktiga grunder för att säkerställa fortsatt överensstämmelse för AI-system på marknaden,

d) informera kommissionen och medlemsstaterna om intyg som den har krävt ska dras tillbaka tillfälligt eller slutgiltigt,

e) förse de nationella behöriga myndigheterna i den medlemsstat där leverantören har sitt säte med all relevant information om de intyg den har krävt ska dras tillbaka tillfälligt eller slutgiltigt. Denna myndighet ska vidta lämpliga åtgärder, om så är nödvändigt för att undvika en potentiell risk för hälsa, säkerhet eller grundläggande rättigheter.

8. Med undantag för intyg som utfärdats på felaktiga grunder, och om ett utseende har återkallats tillfälligt eller begränsats, ska intygen vara giltiga i något av följande fall:

a) Om den anmälande myndigheten inom en månad efter den tillfälliga återkallelsen eller begränsningarna har bekräftat att det inte finns någon risk för hälsa, säkerhet eller grundläggande rättigheter när det gäller intyg som påverkas av den tillfälliga återkallelsen eller begränsningen, och den anmälande myndigheten har angett en tidsfrist för åtgärder som ska leda till att den tillfälliga återkallelsen eller begränsningarna hävs.

b) Om den anmälande myndigheten har bekräftat att inga intyg av betydelse för den tillfälliga återkallelsen ska utfärdas, ändras eller utfärdas på nytt under den tid som den tillfälliga återkallelsen eller begränsningarna gäller, och anger huruvida det anmälda organet har kapacitet att fortsätta att övervaka och ansvara för de befintliga intyg som utfärdats för den period som den tillfälliga återkallelsen eller begränsningarna gäller. Om den anmälande myndigheten *fastställer att det anmälda organet inte har kapacitet att upprätthålla befintliga utfärdade intyg, ska leverantören av det system som omfattas av intyget inom tre månader efter den tillfälliga återkallelsen eller begränsningarna skriftligen bekräfta för de nationella behöriga myndigheterna i den medlemsstat där leverantören har sitt säte att ett annat kvalificerat anmält organ tillfälligt tar på sig det anmälda organets uppgifter att övervaka och fortsätta att ansvara för intygen under den tid som den tillfälliga återkallelsen eller begränsningarna gäller.*

9. Med undantag för intyg som utfärdats på felaktiga grunder och fall där ett utseende har återkallats ska intygen fortsätta att vara giltiga i nio månader under följande omständigheter:

a) Den nationella behöriga myndigheten i den medlemsstat där leverantören av det AI-system som omfattas av intyget har sitt säte har bekräftat att det inte finns någon risk för hälsa, säkerhet eller grundläggande rättigheter i samband med de berörda AI-systemen med hög risk.

b) Ett annat anmält organ har bekräftat skriftligen att det omedelbart kommer att ansvara för bedömningen av dessa AI-system och att det slutför sin bedömning inom tolv månader från det att utseendet har återkallats slutgiltigt.

Under de omständigheter som avses i första stycket får den nationella behöriga myndigheten i den medlemsstat där leverantören av det system som omfattas av intyget har sitt säte förlänga intygens provisoriska giltighet med ytterligare perioder av tre månader i taget, dock längst i tolv månader sammanlagt.

Den nationella behöriga myndighet eller det anmälda organ som tagit på sig de uppgifter som skulle utföras av det anmälda organ som berörs av ändringen av utseendet ska omedelbart informera kommissionen, de andra medlemsstaterna och de andra anmälda organen om ändringen av dessa uppgifter.

Artikel 37

Ifrågasättande av de anmälda organens kompetens

1. Kommissionen ska vid behov undersöka alla fall där det finns skäl att betvivla att ett anmält organ ***har erforderlig kompetens eller att ett anmält organ fortsätter att uppfylla*** kraven i artikel 31 ***och fullgöra sitt tillämpliga ansvar***.

2. Den anmälande myndigheten ska på begäran ge kommissionen all relevant information om anmälan ***eller upprätthållandet av*** det berörda anmälda organets ***kompetens***.

3. Kommissionen ska säkerställa att all ***känslig*** information som den erhåller under sina undersökningar i enlighet med denna artikel behandlas konfidentiellt ***i enlighet med artikel 78***.

4. Om kommissionen konstaterar att ett anmält organ inte uppfyller eller inte längre uppfyller kraven ***för anmälan*** ska den ***informera*** den anmälande medlemsstaten ***om detta och anmoda den*** att vidta erforderliga korrigerande åtgärder, inbegripet att om så är nödvändigt återkalla anmälan ***tillfälligt eller*** slutgiltigt***. Om medlemsstaten inte vidtar erforderliga korrigerande åtgärder får kommissionen genom en genomförandeakt begränsa utseendet eller återkalla det tillfälligt eller slutgiltigt***. Den genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

Artikel 38

Samordning av anmälda organ

1. Kommissionen ska för ***AI-system med hög risk*** säkerställa att lämplig samordning och ett lämpligt samarbete införs mellan de anmälda organ som är verksamma i förfaranden för bedömning av överensstämmelse ▌ i enlighet med denna förordning och att samordningen och samarbetet bedrivs på ett tillfredsställande sätt genom en sektorsspecifik grupp av anmälda organ.

2. Varje ***anmälande myndighet*** ska säkerställa att de organ som den har anmält deltar i arbetet i en grupp som avses i punkt 1 direkt eller genom utsedda representanter.

3. Kommissionen ska se till att det förekommer utbyte av kunskap och bästa praxis mellan de anmälande myndigheterna i medlemsstaterna.

Artikel 39

Organ för bedömning av överensstämmelse i tredje länder

Organ för bedömning av överensstämmelse som inrättats enligt lagstiftningen i ett tredjeland med vilket unionen har ingått ett avtal får bemyndigas att utföra den verksamhet som bedrivs av anmälda organ enligt denna förordning***, förutsatt att de uppfyller kraven i artikel 31 eller säkerställer en likvärdig nivå av överensstämmelse***.

Avsnitt 5

Standarder, bedömning av överensstämmelse, intyg, registrering

Artikel 40

Harmoniserade standarder ***och standardiseringsprodukter***

1. AI-system med hög risk som överensstämmer med harmoniserade standarder eller delar av dem till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning* ***i enlighet med förordning (EU) nr 1025/2012***, ska förutsättas överensstämma med de krav som fastställs i avsnitt 2 i detta kapitel ***eller, i tillämpliga fall, skyldigheterna i*** kapitel IV ***i denna förordning***, i den omfattning som standarderna omfattar dessa krav eller skyldigheter.

2. Kommissionen ska utan onödigt dröjsmål utfärda begäranden om standardisering som omfattar alla krav i avsnitt 2 i detta kapitel och***,*** i tillämpliga fall***, skyldigheterna i*** kapitel ***IV i denna förordning, i enlighet med artikel 10 i förordning (EU) nr 1025/2012. I begäran om standardisering ska det också begäras produkter för rapporterings- och dokumentationsprocesser i syfte att förbättra AI-systemens resursprestanda, t.ex. genom att minska förbrukningen av energi och andra resurser hos AI-systemet med hög risk under dess livscykel, och för energieffektiv utveckling av AI-modeller för allmänna ändamål. När kommissionen utarbetar en begäran om standardisering ska den samråda med nämnden och relevanta berörda parter, inklusive det rådgivande forumet.***

När kommissionen utfärdar en begäran om standardisering till europeiska standardiseringsorganisationer ska den ange att standarderna måste vara tydliga, samstämmiga, inbegripet med de standarder som utvecklas i de olika sektorerna för produkter som omfattas av den befintliga unionslagstiftning om harmonisering som förtecknas i bilaga I, och syfta till att säkerställa att AI-system eller AI-modeller som släpps ut på marknaden eller tas i bruk i unionen uppfyller de relevanta kraven i denna förordning.

Kommissionen ska kräva att de europeiska standardiseringsorganisationerna påvisar att de har gjort sitt yttersta för att uppnå de mål som avses i första och andra styckena i denna punkt i enlighet med artikel 24 i förordning (EU) nr 1025/2012.

3. Deltagarna i standardiseringsprocessen ska sträva efter att främja investeringar och innovation inom AI, inbegripet genom ökad rättssäkerhet, samt konkurrenskraften och tillväxten på unionsmarknaden, och ska bidra till att stärka det globala samarbetet om standardisering och ta hänsyn till befintliga internationella standarder på AI-området som är förenliga med unionens värden, grundläggande rättigheter och intressen, och ska stärka flerpartsstyrningen i syfte att säkerställa en balanserad representation av intressen och ett faktiskt deltagande av alla relevanta berörda parter i enlighet med artiklarna 5, 6 och 7 i förordning (EU) nr 1025/2012.

Artikel 41

Gemensamma specifikationer

1. ***Kommissionen ges befogenhet att anta genomförandeakter om fastställande av gemensamma specifikationer för de krav som anges i*** avsnitt ***2 i detta kapitel eller, i tillämpliga fall, för de*** skyldigheter som anges i kapitel IV, ***om följande villkor är uppfyllda:***

   a) Kommissionen har i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012 begärt att en eller flera europeiska standardiseringsorganisationer ska utarbeta en harmoniserad standard för de krav som anges i avsnitt ***2 i detta kapitel, och***

      i) begäran har inte godtagits av någon av de europeiska standardiseringsorganisationerna, eller

      ii) de harmoniserade standarder som tillgodoser begäran har inte lämnats inom den tidsfrist som fastställts i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012, eller

      iii) de relevanta harmoniserade standarderna tar inte i tillräckligt hög grad hänsyn till frågor som rör de grundläggande rättigheterna, eller

      iv) de harmoniserade standarderna överensstämmer inte med begäran, och

b) ingen hänvisning till harmoniserade standarder som omfattar de krav som avses i avsnitt 2 i denna avdelning har offentliggjorts i Europeiska unionens officiella tidning i enlighet med förordning (EU) nr 1025/2012, och ingen sådan hänvisning förväntas offentliggöras inom rimlig tid.

De genomförandeakter som avses i första stycket i denna punkt ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2, efter samråd med det rådgivande forum som avses i artikel 67.

2. Innan kommissionen utarbetar ett utkast till genomförandeakt ska den informera den kommitté som avses i artikel 22 i förordning (EU) nr 1025/2012 om att den anser att villkoren i punkt 1 i denna artikel är uppfyllda.

3. AI-system med hög risk som överensstämmer med de gemensamma specifikationer som avses i punkt 1***, eller delar av dessa specifikationer,*** ska förutsättas överensstämma med de krav som fastställs i avsnitt 2 i den omfattning som de gemensamma specifikationerna omfattar dessa krav.

4. Om en harmoniserad standard antas av en europeisk standardiseringsorganisation och föreslås för kommissionen för offentliggörande av hänvisningen till den i Europeiska unionens officiella tidning, ska kommissionen bedöma den harmoniserade standarden i enlighet med förordning (EU) nr 1025/2012. När en hänvisning till en harmoniserad standard offentliggörs i Europeiska unionens officiella tidning ska kommissionen upphäva de genomförandeakter som avses i punkt 1, eller delar av dem som omfattar samma krav som anges i avsnitt ***2 i detta kapitel.***

5. Om leverantörer ***av AI-system med hög risk*** inte följer de gemensamma specifikationer som avses i punkt 1 ska de vederbörligen motivera att de har antagit tekniska lösningar som ***uppfyller kraven i*** avsnitt ***2 till en nivå*** som åtminstone är likvärdig med dem.

6. ***Om en medlemsstat anser att en gemensam specifikation inte helt uppfyller kraven i*** avsnitt ***2 ska den underrätta kommissionen om detta med en detaljerad förklaring. Kommissionen ska bedöma denna information och i lämpliga fall ändra genomförandeakten om fastställande av den berörda gemensamma specifikationen.***

Artikel 42

Presumtion om överensstämmelse med vissa krav

1. ▌AI-system med hög risk som har tränats och testats på data som ***återspeglar*** den specifika geografiska, beteendemässiga***, kontextuella eller*** funktionella miljö inom vilken de är avsedda att användas ska förutsättas uppfylla de ***relevanta kraven*** i artikel 10.4.

2. AI-system med hög risk som har certifierats, eller för vilka en försäkran om överensstämmelse har utfärdats inom ramen för en ordning för cybersäkerhetscertifiering i enlighet med förordning (EU) 2019/881, och till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning*, ska förutsättas överensstämma med de cybersäkerhetskrav som anges i artikel 15 i den här förordningen, förutsatt att cybersäkerhetscertifikatet eller försäkran om överensstämmelse eller delar därav omfattar dessa krav.

Artikel 43

Bedömning av överensstämmelse

1. För AI-system med hög risk som förtecknas i punkt 1 i bilaga III ska leverantören, när den vill visa att ett AI-system med hög risk uppfyller kraven i avsnitt 2 och den har tillämpat de harmoniserade standarder som avses i artikel 40 eller, i tillämpliga fall, de gemensamma specifikationer som avses i artikel 41, ***välja*** ett av följande förfaranden för bedömning av överensstämmelse grundat på

   a) intern kontroll som avses i bilaga VI, ***eller***

   b) en bedömning av kvalitetsstyrningssystemet och en bedömning av den tekniska dokumentationen, med deltagande av ett anmält organ, som avses i bilaga VII.

▌När leverantören vill visa att ett AI-system med hög risk uppfyller de krav som fastställs i avsnitt 2 ***ska*** leverantören ***följa det förfarande för bedömning av överensstämmelse som fastställs i bilaga VII i följande fall:***

   a) De harmoniserade standarder som avses i artikel 40 ▌ saknas, och de gemensamma specifikationer som avses i artikel 41 är inte tillgängliga***.***

   b) Leverantören ***har inte tillämpat eller har endast tillämpat en del av den harmoniserade standarden.***

   c) De gemensamma specifikationer som avses i led a finns men leverantören har inte tillämpat dem.

   d) En eller flera av de harmoniserade standarder som avses i led a har offentliggjorts med en begränsning och endast för den del av standarden som begränsades.

För det förfarande för bedömning av överensstämmelse som avses i bilaga VII får leverantören välja vilket av de anmälda organen som helst. Om AI-systemet med hög risk är avsett att tas i bruk av brottsbekämpande myndigheter, invandringsmyndigheter eller asylmyndigheter eller av unionens institutioner, organ eller byråer ska dock den marknadskontrollmyndighet som avses i artikel 74.8 eller 74.9, beroende på vad som är tillämpligt, fungera som anmält organ.

2. För de AI-system med hög risk som avses i punkterna 2–8 i bilaga III ▌ ska leverantörerna följa det förfarande för bedömning av överensstämmelse grundat på intern kontroll som avses i bilaga VI, vilket inte föreskriver att ett anmält organ ska delta. ▌

3. För AI-system med hög risk som omfattas av den unionslagstiftning om harmonisering som förtecknas i avsnitt A i bilaga I ska leverantören följa det relevanta förfarande för bedömning av överensstämmelse som krävs enligt dessa rättsakter. Kraven i avsnitt 2 i detta kapitel ska tillämpas på de AI-systemen med hög risk och ska ingå i den bedömningen. Punkterna 4.3, 4.4 och 4.5 och punkt 4.6 femte stycket i bilaga VII ska också tillämpas.

Vid denna bedömning ska anmälda organ som har anmälts i enlighet med de rättsakterna ha rätt att kontrollera att AI-systemen med hög risk överensstämmer med kraven i avsnitt 2, förutsatt att dessa anmälda organs överensstämmelse med kraven i artikel 31.4, 31.10 och 31.11 har bedömts i samband med anmälningsförfarandet inom ramen för dessa rättsakter.

Om en rättsakt som förtecknas i avsnitt A i bilaga I gör det möjligt för produkttillverkaren att välja att inte delta i en tredjepartsbedömning av överensstämmelse får tillverkaren, om den har tillämpat alla harmoniserade standarder som omfattar alla relevanta krav, använda detta alternativ endast om den också har tillämpat harmoniserade standarder eller, i tillämpliga fall, de gemensamma specifikationer som avses i artikel 41, som omfattar de krav som anges i avsnitt 2 i detta kapitel.

4. AI-system med hög risk ***som redan har varit föremål för ett förfarande för bedömning av överensstämmelse*** ska genomgå ett nytt förfarande för bedömning av överensstämmelse i fall av en väsentlig ändring, oavsett om det ändrade systemet är avsett att distribueras vidare eller fortsätter att användas av den nuvarande ***spridaren***.

   När det gäller AI-system med hög risk som fortsätter att lära sig efter att det har släppts ut på marknaden eller tagits i bruk, ska sådana ändringar av AI-systemet med hög risk och dess prestanda som leverantören på förhand har fastställt vid tidpunkten för den inledande bedömningen av överensstämmelse och som är en del av den information som ingår i den tekniska dokumentation som avses i punkt 2 f i bilaga IV inte utgöra en väsentlig ändring.

5. Kommissionen ska anta delegerade akter i enlighet med artikel 97 för att uppdatera bilagorna VI och VII på ▌ grund av tekniska framsteg.

6. Kommissionen ska anta delegerade akter i enlighet med artikel 97 för att ändra punkterna 1 och 2 i denna artikel i syfte att låta de AI-system med hög risk som avses i punkterna 2–8 i bilaga III omfattas av det förfarande för bedömning av överensstämmelse som avses i bilaga VII eller delar därav. Kommissionen ska anta sådana delegerade akter med beaktande av hur ändamålsenligt förfarandet för bedömning av överensstämmelse grundat på intern kontroll enligt bilaga VI är när det gäller att förebygga eller minimera de risker för hälsa, säkerhet och skyddet av grundläggande rättigheter som sådana system medför samt vilken tillgång det finns till tillräcklig kapacitet och tillräckliga resurser bland anmälda organ.

Artikel 44

Intyg

1. De intyg som de anmälda organen utfärdar i enlighet med bilaga VII ska vara upprättade på ***ett språk som är lätt att förstå*** för de ***relevanta myndigheterna i den*** medlemsstat där det anmälda organet är etablerat.

2. Intyg ska gälla under den tid som anges i dem och högst i fem år ***för AI-system som omfattas av bilaga I, och fyra år för AI-system som omfattas av bilaga III***. På begäran av leverantören får intygets giltighet förlängas med högst fem år i taget ***för AI-system som omfattas av bilaga I, och fyra år för AI-system som omfattas av bilaga III,*** på grundval av en ny bedömning i enlighet med det tillämpliga förfarandet för bedömning av överensstämmelse. ***Eventuella tillägg till ett intyg ska vara giltiga, förutsatt att intyget är giltigt.***

3. Om ett anmält organ konstaterar att ett AI-system inte längre uppfyller de krav som fastställs i avsnitt 2, ska det, med beaktande av proportionalitetsprincipen, tillfälligt eller slutligt återkalla det utfärdade intyget eller införa begränsningar för det, om det inte säkerställs att dessa krav uppfylls genom att systemleverantören vidtar lämpliga korrigerande åtgärder inom en rimlig tidsgräns som fastställts av det anmälda organet. Det anmälda organet ska motivera sitt beslut.

   Det ska finnas ett förfarande för överklagande av de anmälda organens beslut, inbegripet när det gäller utfärdade intyg om överensstämmelse.

Artikel 45

De anmälda organens informationsskyldighet

1. Anmälda organ ska informera den anmälande myndigheten om följande:

a) Alla eventuella unionsintyg om bedömning av teknisk dokumentation, tillägg till dessa intyg samt godkännanden av kvalitetsstyrningssystem som utfärdats i enlighet med kraven i bilaga VII.

b) Eventuella avslag, begränsningar, tillfälliga återkallelser eller tillbakadraganden av ett unionsintyg om bedömning av teknisk dokumentation eller av ett godkännande av kvalitetsstyrningssystem som utfärdats i enlighet med kraven i bilaga VII.

c) Omständigheter som inverkar på omfattningen av eller villkoren för anmälan.

d) Begäranden från marknadskontrollmyndigheterna om information om bedömningar av överensstämmelse.

e) På begäran, bedömningar av överensstämmelse som gjorts inom ramen för anmälan och all annan verksamhet, inklusive gränsöverskridande verksamhet och underentreprenad.

2. Varje anmält organ ska underrätta de övriga anmälda organen om följande:

   a) Godkännanden av kvalitetsstyrningssystem som det har vägrat utfärda eller tillfälligt återkallat eller dragit tillbaka och, på begäran, godkännanden av kvalitetsstyrningssystem som det har utfärdat.

   b) Unionsintyg om bedömning av teknisk dokumentation eller tillägg till dessa intyg som det har avslagit, tillfälligt återkallat eller dragit tillbaka eller på annat sätt begränsat och, på begäran, de intyg och/eller tillägg till dessa som det har utfärdat.

3. Varje anmält organ ska ge de andra anmälda organ som utför liknande bedömningar av överensstämmelse avseende samma ***typer av AI-system*** relevant information om frågor som rör negativa och, på begäran, positiva resultat av bedömningar av överensstämmelse.

4. De skyldigheter som avses i punkterna 1, 2 och 3 i denna artikel ska fullgöras i enlighet med artikel 78.

Artikel 46

Undantag från förfarandena för bedömning av överensstämmelse

1. Genom undantag från artikel 43 ***och på vederbörligen motiverad begäran*** får varje marknadskontrollmyndighet, av exceptionella skäl som rör allmän säkerhet eller skydd av människors liv och hälsa, miljöskydd eller skydd av viktiga industriella och infrastrukturella tillgångar, tillåta att specifika AI-system med hög risk släpps ut på marknaden eller tas i bruk inom den berörda medlemsstatens territorium. Tillståndet ska gälla under en begränsad period ▌, medan de nödvändiga förfarandena för bedömning av överensstämmelse genomförs, ***med beaktande av de exceptionella skäl som motiverar undantaget***. Dessa förfaranden ska slutföras utan onödigt dröjsmål.

2. I en vederbörligen motiverad brådskande situation får brottsbekämpande myndigheter eller civilskyddsmyndigheter av exceptionella skäl som rör allmän säkerhet eller vid ett specifikt, betydande och överhängande hot mot fysiska personers liv eller fysiska säkerhet ta ett specifikt AI-system med hög risk i bruk utan det tillstånd som avses i punkt 1, förutsatt att ett sådant tillstånd begärs under eller efter användningen utan onödigt dröjsmål. Om det tillstånd som avses i punkt 1 avslås ska användningen av AI-systemet med hög risk avbrytas med omedelbar verkan, och alla resultat och utdata från sådan användning ska omedelbart kasseras.

3. Det tillstånd som avses i punkt 1 ska utfärdas endast om marknadskontrollmyndigheten konstaterar att AI-systemet med hög risk uppfyller kraven i avsnitt 2. Marknadskontrollmyndigheten ska informera kommissionen och de andra medlemsstaterna om eventuella tillstånd som utfärdats i enlighet med punkt 1. ***Denna skyldighet ska inte omfatta känsliga operativa uppgifter som rör de brottsbekämpande myndigheternas verksamhet.***

4. Tillståndet ska anses vara motiverat om ingen medlemsstat eller kommissionen har gjort någon invändning inom 15 kalenderdagar från mottagandet av den information som avses i punkt 3 om ett tillstånd utfärdat av en marknadskontrollmyndighet i en medlemsstat i enlighet med punkt 1.

5. Om en medlemsstat inom 15 kalenderdagar från mottagandet av den anmälan som avses i punkt 3 gör en invändning mot ett tillstånd som utfärdats av en marknadskontrollmyndighet i en annan medlemsstat, eller om kommissionen anser att tillståndet strider mot unionslagstiftningen, eller att medlemsstatens slutsats om systemets överensstämmelse som avses i punkt 3 är ogrundad, ska kommissionen utan dröjsmål inleda samråd med den berörda medlemsstaten. De berörda operatörerna ska rådfrågas och ha möjlighet att framföra sina åsikter. Med beaktande av detta ska kommissionen besluta om tillståndet är motiverat eller inte. Kommissionen ska rikta sitt beslut till den berörda medlemsstaten och till de berörda operatörerna.

6. Om kommissionen anser att tillståndet är omotiverat ska det dras tillbaka av den berörda medlemsstatens marknadskontrollmyndighet.

7. För AI-system med hög risk ***som är relaterade till produkter*** som omfattas av ***den unionslagstiftning om harmonisering som förtecknas i avsnitt A i bilaga I ska endast*** de ***undantag från bedömningen av överensstämmelse som fastställs i den unionslagstiftningen om harmonisering tillämpas***.

Artikel 47

EU-försäkran om överensstämmelse

1. Leverantören ska upprätta en skriftlig ***maskinläsbar, fysisk eller elektroniskt undertecknad*** EU-försäkran om överensstämmelse för varje AI-system ***med hög risk*** och kunna uppvisa den för de nationella behöriga myndigheterna i tio år efter det att AI-systemet ***med hög risk*** har släppts ut på marknaden eller tagits i bruk. I EU-försäkran om överensstämmelse ska det anges för vilket AI-system ***med hög risk*** den har ***upp***rättats. ***En*** kopia av EU-försäkran om överensstämmelse ska på begäran ***lämnas in*** till de berörda nationella behöriga myndigheterna.

2. I EU-försäkran om överensstämmelse ska det anges att det berörda AI-systemet med hög risk uppfyller kraven i avsnitt 2. EU-försäkran om överensstämmelse ska innehålla den information som anges i bilaga V och ska översättas till ***ett språk som är lätt att förstå*** för de ***nationella behöriga myndigheterna i de*** medlemsstater där AI-systemet med hög risk ***släpps ut på marknaden eller*** tillhandahålls.

3. Om AI-system med hög risk omfattas av annan unionslagstiftning om harmonisering som också kräver en EU-försäkran om överensstämmelse ska en enda EU-försäkran om överensstämmelse upprättas med avseende på all unionsrätt som är tillämplig på AI-systemet med hög risk. Försäkran ska innehålla all information som krävs för att identifiera vilken unionslagstiftning om harmonisering som försäkran gäller.

4. Genom att upprätta EU-försäkran om överensstämmelse ska leverantören ta på sig ansvaret för att kraven i avsnitt 2 uppfylls. Leverantören ska hålla EU-försäkran om överensstämmelse uppdaterad på lämpligt sätt.

5. Kommissionen ska anta delegerade akter i enlighet med artikel 97 i syfte att uppdatera innehållet i den EU-försäkran om överensstämmelse som anges i bilaga V för att introducera element som blir nödvändiga på grund av tekniska framsteg.

Artikel 48

CE-märkning

1. CE-märkningen ska ***omfattas*** av de ***allmänna principer som fastställs i artikel 30 i förordning (EG) nr 765/2008***.

2. ***För AI-system med hög risk som tillhandahålls digitalt ska en digital CE-märkning användas endast om den lätt kan nås via det gränssnitt från vilket det systemet är tillgängligt eller via en lättillgänglig maskinläsbar kod eller andra elektroniska medel.***

3. CE-märkningen ***ska anbringas på AI-system med hög risk så att den är synlig, läsbar och outplånlig. Om detta inte är möjligt eller lämpligt på grund av arten av AI-system med hög risk,*** ska ***märkningen anbringas*** på ***förpackningen eller den medföljande dokumentationen, beroende på vad som är lämpligt***.

4. CE-märkningen ska i tillämpliga fall åtföljas av identifikationsnumret för det anmälda organ som ansvarar för de förfaranden för bedömning av överensstämmelse som föreskrivs i artikel 43. ***Det anmälda organets*** identifikationsnummer ***ska anbringas av organet självt eller, enligt organets anvisningar, av leverantören eller av leverantörens ombud. Identifikationsnumret*** ska också anges i reklammaterial där det nämns att AI-systemet med hög risk uppfyller kraven för CE-märkning.

5. ***Om AI-system med hög risk omfattas av annan unionsrätt som också föreskriver anbringande av CE-märkning ska CE-märkningen visa att AI-systemet med hög risk också uppfyller kraven i den andra lagstiftningen.***

Artikel 49

Registrering

1. Innan ett AI-system med hög risk ***som förtecknas i bilaga III, med undantag för AI-system med hög risk*** som avses i ***punkt 2 i bilaga III,*** släpps ut på marknaden eller tas i bruk ska leverantören eller, i tillämpliga fall, ombudet registrera ***sig självt och systemet*** i den EU-databas som avses i artikel 71.

2. ***Innan ett AI-system för vilket leverantören har fastställt att det inte utgör hög risk i enlighet med artikel 6.3 släpps ut på marknaden eller tas i bruk ska leverantören eller, i tillämpliga fall, ombudet registrera sig självt och detta system i den EU-databas som avses i artikel 71.***

3. ***Innan ett AI-system med hög risk som förtecknas i bilaga III, med undantag för AI-system med hög risk som förtecknas i punkt 2 i bilaga III, tas i bruk eller används, ska spridare som är offentliga myndigheter, byråer eller organ eller personer som agerar på deras vägnar, registrera sig, välja systemet och registrera dess användning i den EU-databas som avses i artikel 71.***

4. ***För AI-system med hög risk som avses i punkterna 1, 6 och 7 i bilaga III, på områdena brottsbekämpning, migration, asyl och gränskontrollförvaltning, ska den registrering som avses i punkterna 1, 2 och 3 i denna artikel vara i en säkrad, icke-offentlig del av den EU-databas som avses i artikel 71 och ska, beroende på vad som är tillämpligt, omfatta endast följande information som avses i***

   a) avsnitt A, punkterna 1–10, i bilaga VIII, med undantag för punkterna 5a, 7 och 8,

   b) avsnitt C, punkterna 1–3***, i bilaga VIII,***

   c) avsnitt B, ***punkterna 1–5, och punkterna 8 och 9 i bilaga VIII,***

   d) punkterna 1–3, och punkt 5, i bilaga IX.

   Endast kommissionen och de nationella myndigheter som avses i artikel 74.8 ska ha tillgång till de begränsade delar av EU-databasen som förtecknas i första stycket i denna punkt.

5. De AI-system med hög risk som avses i punkt 2 i bilaga III ska registreras på nationell nivå.

KAPITEL IV
TRANSPARENSSKYLDIGHETER FÖR *LEVERANTÖRER OCH SPRIDARE AV* VISSA AI-SYSTEM

Artikel 50

Transparensskyldigheter för leverantörer och användare av vissa AI-system

1. Leverantörer ska säkerställa att AI-system som är avsedda att interagera ***direkt*** med fysiska personer utformas och utvecklas på ett sådant sätt att ***de berörda*** fysiska personerna informeras om att de interagerar med ett AI-system, såvida detta inte är uppenbart ***för en fysisk person som är normalt informerad och skäligen uppmärksam och medveten, med beaktande av*** användningens omständigheter och sammanhang. Denna skyldighet ska inte gälla AI-system som enligt lag får upptäcka, förebygga, utreda eller lagföra brott, ***med förbehåll för lämpliga garantier för tredje mans rättigheter och friheter,*** såvida inte dessa system är tillgängliga för allmänheten för att anmäla ett brott.

2. ***Leverantörer av AI-system, inbegripet AI-system för allmänna ändamål, som genererar syntetiskt ljud-, bild-, video- eller textinnehåll ska säkerställa att AI-systemets utdata är märkta i ett maskinläsbart format och kan upptäckas som artificiellt genererade eller manipulerade. Leverantörerna ska säkerställa att deras tekniska lösningar är effektiva, interoperabla, robusta och tillförlitliga i den mån det är tekniskt möjligt, med beaktande av särdragen och begränsningarna hos olika typer av innehåll, genomförandekostnaderna och teknikens allmänt erkända ståndpunkt, vilket kan återspeglas i relevanta tekniska standarder. Denna skyldighet ska inte gälla i den mån AI-systemen utför en hjälpfunktion för vanlig redigering eller inte väsentligt ändrar de indata som tillhandahålls av spridaren eller deras semantik, eller om systemen enligt lag får upptäcka, förebygga, utreda eller lagföra brott.***

3. ***Spridare*** av ett system för känsloigenkänning eller ett system för biometrisk kategorisering ska informera de fysiska personer som exponeras för systemet om systemets drift, ***och ska behandla personuppgifter i enlighet med förordningarna (EU) 2016/679 och (EU) 2018/1725 och direktiv (EU) 2016/680, beroende på vad som är tillämpligt***. Denna skyldighet ska inte gälla AI-system som används för biometrisk ***kategorisering och känsloigenkänning*** och som enligt lag får upptäcka, förebygga eller utreda brott, ***med förbehåll för lämpliga garantier för tredje mans rättigheter och friheter, och i överensstämmelse med unionsrätten***.

4. ***Spridare*** av ett AI-system som genererar eller manipulerar bild-, ljud- eller videoinnehåll ***som utgör en deepfake ska upplysa om att innehållet har genererats artificiellt eller manipulerats. Denna skyldighet ska inte gälla om användningen enligt lag är tillåten för att upptäcka, förebygga, utreda eller lagföra brott. Om innehållet utgör en del av ett uppenbart konstnärligt, kreativt, satiriskt eller skönlitterärt liknande verk eller program, ska de transparenskrav som anges i denna punkt begränsas till att upplysa om förekomsten av sådant*** genererat eller manipulerat ***innehåll på ett lämpligt sätt som inte hindrar visningen eller åtnjutandet av verket***.

Spridare av ett AI-system som genererar eller manipulerar text som offentliggörs i syfte att informera allmänheten om frågor av allmänt intresse ska upplysa om att texten har genererats artificiellt eller manipulerats. Denna skyldighet ska inte gälla om användningen enligt lag är tillåten för att upptäcka, förebygga, utreda eller lagföra brott eller ***om det AI-genererade innehållet har genomgått en process med mänsklig granskning eller redaktionell kontroll och om en fysisk eller juridisk person bär det redaktionella ansvaret*** för ***offentliggörandet av innehållet***.

5. ***Den information som avses i punkterna 1–4 ska lämnas till de berörda fysiska personerna på ett tydligt och urskiljbart sätt senast vid tidpunkten för den första interaktionen eller exponeringen. Informationen ska uppfylla de tillämpliga tillgänglighetskraven.***

6. Punkterna 1–4 ska inte påverka de krav och skyldigheter som fastställs i kapitel III, ***och ska inte påverka andra transparensskyldigheter som fastställs i unionsrätten eller nationell rätt för spridare av AI-system.***

7. ***AI-byrån ska uppmuntra och underlätta utarbetandet av förfarandekoder på unionsnivå för att underlätta ett effektivt genomförande av skyldigheterna avseende upptäckt och märkning av artificiellt skapat eller manipulerat innehåll. Kommissionen ges befogenhet att anta genomförandeakter för att godkänna dessa förfarandekoder i enlighet med förfarandet i artikel 56.6, 56.7 och 56.8. Om kommissionen anser att förfarandekoden inte är lämplig får den anta en genomförandeakt som specificerar gemensamma regler för genomförandet av dessa skyldigheter i enlighet med det granskningsförfarande som fastställs i artikel 98.2.***

KAPITEL V
AI-MODELLER FÖR ALLMÄNNA ÄNDAMÅL

Avsnitt 1
Klassificeringsregler

Artikel 51
Klassificering av AI-modeller för allmänna ändamål som AI-modeller för allmänna ändamål med systemrisk

1. En AI-modell för allmänna ändamål ska klassificeras som en AI-modell för allmänna ändamål med systemrisk om den uppfyller något av följande krav:

a) Den har kapacitet med hög påverkansgrad som utvärderats på grundval av lämpliga tekniska verktyg och metoder, inbegripet indikatorer och riktmärken.

b) Den har, baserat på ett beslut av kommissionen, på eget initiativ eller efter en kvalificerad varning från den vetenskapliga panelen, kapacitet eller inverkan som motsvarar den som avses i led a med beaktande av kriterierna i bilaga XIII.

2. En AI-modell för allmänna ändamål ska förutsättas ha kapacitet med hög påverkansgrad i enlighet med punkt 1 a om den sammanlagda beräkningsmängd som används för dess träning mätt i flyttalsberäkningar är större än 10^25.

3. Kommissionen ska anta delegerade akter i enlighet med artikel 97 för att ändra de tröskelvärden som anges i punkterna 2 och 3 i denna artikel samt för att komplettera riktmärken och indikatorer mot bakgrund av den tekniska utvecklingen, såsom algoritmiska förbättringar eller ökad hårdvarueffektivitet, när så krävs för att dessa tröskelvärden ska återspegla den senaste tekniken.

Artikel 52

Förfarande

1. Om en AI-modell för allmänna ändamål uppfyller det krav som avses i artikel 51.1 a ska den berörda leverantören underrätta kommissionen utan dröjsmål och under alla omständigheter inom två veckor efter att kravet är uppfyllt eller det blir känt att det kommer att uppfyllas. Anmälan ska innehålla den information som krävs för att visa att det relevanta kravet har uppfyllts. Om kommissionen får kännedom om en AI-modell för allmänna ändamål som medför systemrisker och som den inte har underrättats om får den besluta att klassificera den som en modell med systemrisk.

2. Leverantören av en AI-modell för allmänna ändamål som uppfyller det krav som avses i artikel 51.1 a får tillsammans med sin anmälan lägga fram tillräckligt underbyggda argument för att visa att AI-modellen för allmänna ändamål, även om den uppfyller det kravet, i detta undantagsfall inte medför systemrisker på grund av sina särskilda egenskaper och därför inte bör klassificeras som en AI-modell för allmänna ändamål med systemrisk.

3. Om kommissionen konstaterar att de argument som lagts fram i enlighet med punkt 2 inte är tillräckligt underbyggda och att den berörda leverantören inte har kunnat visa att AI-modellen för allmänna ändamål, på grund av sina särskilda egenskaper, inte medför systemrisker ska den avvisa dessa argument, och AI-modellen för allmänna ändamål ska anses vara en AI-modell för allmänna ändamål med systemrisk.

4. Kommissionen får, på eget initiativ eller efter en kvalificerad varning från den vetenskapliga panelen i enlighet med artikel 90.1 a, klassificera en AI-modell för allmänna ändamål som en AI-modell för allmänna ändamål med systemrisk, på grundval av kriterierna i bilaga XIII.

Kommissionen ska anta delegerade akter i enlighet med artikel 97 för att specificera och uppdatera kriterierna i bilaga XIII.

5. På motiverad begäran av en leverantör vars modell har klassificerats som en AI-modell för allmänna ändamål med systemrisk i enlighet med punkt 4 ska kommissionen beakta begäran och kan besluta att ompröva huruvida AI-modellen för allmänna ändamål fortfarande kan anses medföra systemrisker på grundval av kriterierna i bilaga XIII. En sådan begäran ska innehålla objektiva, detaljerade och nya skäl som har tillkommit sedan klassificeringsbeslutet fattades. Leverantörer får begära en ny bedömning tidigast sex månader efter klassificeringsbeslutet. Om kommissionen efter sin nya bedömning beslutar att behålla klassificeringen som en AI-modell för allmänna ändamål med systemrisk får leverantörerna begära en ny bedömning tidigast sex månader efter det beslutet.

6. Kommissionen ska säkerställa att en förteckning över AI-modeller för allmänna ändamål med systemrisk offentliggörs och ska hålla denna förteckning uppdaterad, utan att det påverkar behovet av att respektera och skydda immateriella rättigheter och konfidentiell affärsinformation eller företagshemligheter i enlighet med unionsrätten och nationell rätt.

Avsnitt 2

Skyldigheter för leverantörer av AI-modeller för allmänna ändamål

Artikel 53

Skyldigheter för leverantörer av AI-modeller för allmänna ändamål

1. Leverantörer av AI-modeller för allmänna ändamål ska

a) utarbeta och uppdatera den tekniska dokumentationen för modellen, inbegripet tränings- och testningsförfarandet samt resultaten av utvärderingen, som åtminstone ska innehålla de uppgifter som anges i bilaga XI, i syfte att på begäran lägga fram den för AI-byrån och de nationella behöriga myndigheterna,

b) utarbeta, uppdatera och göra information och dokumentation tillgänglig för leverantörer av AI-system som avser att integrera AI-modellen för allmänna ändamål i sina AI-system; utan att det påverkar behovet av att respektera och skydda immateriella rättigheter och konfidentiell affärsinformation eller företagshemligheter i enlighet med unionsrätten och nationell rätt ska informationen och dokumentationen

i) göra det möjligt för leverantörer av AI-system att ha en god förståelse av kapaciteten och begränsningarna hos AI-modellen för allmänna ändamål och att fullgöra sina skyldigheter enligt denna förordning, och

ii) minst innehålla de uppgifter som anges i bilaga XII,

c) införa en policy för att följa unionens upphovsrättslagstiftning, och i synnerhet för att identifiera och efterleva, inbegripet med hjälp av den senaste tekniken, ett förbehåll för rättigheter som uttryckts i enlighet med artikel 4.3 i direktiv (EU) 2019/790,

d) utarbeta och göra en tillräckligt detaljerad sammanfattning av det innehåll som använts för träning av AI-modellen för allmänna ändamål allmänt tillgänglig, i enlighet med en mall som tillhandahålls av AI-byrån.

2. De skyldigheter som anges i punkt 1 a och b ska inte tillämpas på leverantörer av AI-modeller som släpps ut med en fri och öppen licens som möjliggör åtkomst, användning, ändring och distribution av modellen, och vars parametrar, inbegripet vikter, information om modellarkitekturen och information om modellanvändning, görs allmänt tillgängliga. Detta undantag ska inte tillämpas på AI-modeller för allmänna ändamål med systemrisk.

3. Leverantörer av AI-modeller för allmänna ändamål ska vid behov samarbeta med kommissionen och de nationella behöriga myndigheterna vid utövandet av sin behörighet och sina befogenheter enligt denna förordning.

4. Leverantörer av AI-modeller för allmänna ändamål får förlita sig på förfarandekoder i den mening som avses i artikel 56 för att visa att de fullgjort de skyldigheter som anges i punkt 1 i denna artikel, till dess att en harmoniserad standard har offentliggjorts. Leverantörer som följer en europeisk harmoniserad standard ska förutsättas uppfylla de skyldigheter som anges i punkt 1 i denna artikel. Leverantörer av AI-modeller för allmänna ändamål som inte följer en godkänd förfarandekod ska uppvisa alternativa lämpliga sätt att uppfylla kraven, vilka ska godkännas av kommissionen.

5. I syfte att underlätta efterlevnaden av bilaga XI, särskilt punkt 2 d och e, ska kommissionen anta delegerade akter i enlighet med artikel 97 för att närmare specificera mät- och beräkningsmetoder i syfte att möjliggöra jämförbar och verifierbar dokumentation.

6. Kommissionen ska anta delegerade akter i enlighet med artikel 97.2 för att ändra bilagorna XI och XII mot bakgrund av den pågående tekniska utvecklingen.

7. All information eller dokumentation som har erhållits enligt denna artikel, inbegripet företagshemligheter, ska behandlas i enlighet med de konfidentialitetskrav som anges i artikel 78.

Artikel 54

Ombud för leverantörer av AI-modeller för allmänna ändamål

1. Innan leverantörer som är etablerade i tredjeländer släpper ut en AI-modell för allmänna ändamål på unionsmarknaden ska de genom skriftlig fullmakt utse ett ombud som är etablerat i unionen.

2. Leverantören ska göra det möjligt för sitt ombud att utföra de uppgifter som anges i fullmakten från leverantören.

2. Ombudet ska utföra de uppgifter som anges i fullmakten från leverantören. Ombudet ska på begäran lämna en kopia av fullmakten till AI-byrån på ett av unionsinstitutionernas officiella språk. Vid tillämpningen av denna förordning ska fullmakten ge ombudet befogenhet att utföra följande uppgifter:

a) Kontrollera att den tekniska dokumentation som anges i bilaga XI har upprättats och att alla skyldigheter som avses i artiklarna 53 och, i tillämpliga fall, 55 har fullgjorts av leverantören.

b) Kunna uppvisa en kopia av den tekniska dokumentation som anges i bilaga XI för AI-byrån och de nationella behöriga myndigheterna under en period på 10 år efter det att AI-modellen för allmänna ändamål har släppts ut på marknaden, och bevara aktuella kontaktuppgifter för den leverantör som utsett ombudet.

c) På motiverad begäran förse AI-byrån med all information och dokumentation, inbegripet den som avses i led b, som krävs för att visa att den fullgör skyldigheterna i detta kapitel.

d) Samarbeta med AI-byrån och nationella behöriga myndigheter, på motiverad begäran, när det gäller alla åtgärder som de senare vidtar med avseende på en AI-modell för allmänna ändamål med systemrisk, inbegripet när modellen är integrerad i AI-system som släpps ut på marknaden eller tas i bruk i unionen.

3. Fullmakten ska ge ombudet befogenhet att utöver eller i stället för leverantören stå till förfogande inför AI-byrån eller de nationella behöriga myndigheterna, i alla frågor som rör efterlevnaden av denna förordning.

4. Ombudet ska säga upp fullmakten om denne anser eller har skäl att tro att leverantören agerar i strid med sina skyldigheter enligt denna förordning. I sådana fall ska det också omedelbart informera AI-byrån om uppsägningen av fullmakten och skälen till detta.

5. Den skyldighet som anges i denna artikel ska inte tillämpas på leverantörer av AI-modeller för allmänna ändamål som släpps ut med en fri licens med öppen källkod som möjliggör åtkomst, användning, ändring och distribution av modellen, och vars parametrar, inbegripet vikter, information om modellarkitekturen och information om modellanvändning, görs allmänt tillgängliga, såvida inte AI-modellen för allmänna ändamål medför systemrisker.

Avsnitt 3

Skyldigheter för leverantörer av AI-modeller för allmänna ändamål med systemrisk

Artikel 55

Skyldigheter för leverantörer av AI-modeller för allmänna ändamål med systemrisk

1. Utöver de skyldigheter som förtecknas i artikel 53 ska leverantörer av AI-modeller för allmänna ändamål med systemrisk

a) genomföra utvärderingar av modeller i enlighet med standardiserade protokoll och verktyg som återspeglar den aktuella tekniska nivån, inbegripet genomförande och dokumentation av antagonistisk testning av modellen i syfte att identifiera och minska systemrisker,

b) bedöma och minska eventuella systemrisker på unionsnivå, inbegripet källorna till dem, som kan härröra från utveckling, utsläppande på marknaden eller användning av AI-modeller för allmänna ändamål med systemrisk,

c) bevaka, dokumentera och utan onödigt dröjsmål rapportera till AI-byrån och, i förekommande fall, till nationella behöriga myndigheter, relevant information om allvarliga incidenter och möjliga korrigerande åtgärder för att hantera dem,

d) säkerställa en lämplig nivå av cybersäkerhetsskydd för AI-modellen för allmänna ändamål med systemrisk och modellens fysiska infrastruktur.

2. Leverantörer av AI-modeller för allmänna ändamål med systemrisk får förlita sig på förfarandekoder i den mening som avses i artikel *56 för att visa att de fullgjort de skyldigheter som anges i punkt 1 i denna artikel, till dess att en harmoniserad standard har offentliggjorts. Leverantörer som följer en europeisk harmoniserad standard ska förutsättas uppfylla de skyldigheter som anges i punkt 1 i denna artikel. Leverantörer av AI-modeller för allmänna ändamål med systemrisk som inte följer en godkänd förfarandekod ska uppvisa alternativa lämpliga sätt att uppfylla kraven, vilka ska godkännas av kommissionen.*

3. All information eller dokumentation som har erhållits enligt denna artikel, inbegripet företagshemligheter, ska behandlas i enlighet med de konfidentialitetskrav som anges i artikel 78.

Artikel 56

Förfarandekoder

1. AI-byrån ska uppmuntra och underlätta utarbetandet av förfarandekoder på unionsnivå för att bidra till en korrekt tillämpning av denna förordning, med beaktande av internationella strategier.

2. AI-byrån och nämnden ska sträva efter att säkerställa att förfarandekoderna åtminstone omfattar de skyldigheter som fastställs i artiklarna 53 och 55, inbegripet följande aspekter:

a) Metoder för att säkerställa att den information som avses i artikel 53.1 a och b *hålls uppdaterad mot bakgrund av marknadsutvecklingen och den tekniska utvecklingen.*

b) Lämplig detaljnivå för sammanfattningen av det innehåll som använts för träning.

c) Identifiering av systemriskernas typ och art på unionsnivå, inbegripet källorna till dem, när så är lämpligt.

d) Åtgärderna, förfarandena och formerna för bedömning och hantering av systemrisker på unionsnivå, inbegripet dokumentationen av dessa, som ska stå i proportion till riskerna samt ta hänsyn till deras allvar och sannolikhet och till de särskilda utmaningarna med att hantera dessa risker mot bakgrund av de möjliga sätt på vilka sådana risker kan uppstå och bli verklighet längs AI-värdekedjan.

3. AI-byrån får uppmana alla leverantörer av AI-modeller för allmänna ändamål, samt relevanta nationella behöriga myndigheter, att delta i utarbetandet av förfarandekoder. Det civila samhällets organisationer, industrin, den akademiska världen och andra berörda parter, såsom leverantörer i efterföljande led och oberoende experter, får stödja processen.

4. AI-byrån och nämnden ska sträva efter att säkerställa att förfarandekoderna innehåller tydligt angivna specifika mål samt åtaganden eller åtgärder, inbegripet nyckelprestationsindikatorer när så är lämpligt, för att säkerställa att dessa mål uppnås, och att de tar vederbörlig hänsyn till alla intressenters, inbegripet berörda personers, behov och intressen på unionsnivå.

5. AI-byrån ska sträva efter att säkerställa att deltagarna i förfarandekoderna regelbundet rapporterar till AI-byrån om genomförandet av åtagandena samt de åtgärder som vidtagits och deras resultat, även i förhållande till nyckelprestationsindikatorerna när så är lämpligt. Nyckelprestationsindikatorer och rapporteringsåtaganden ska återspegla skillnader i storlek och kapacitet mellan olika deltagare.

6. AI-byrån och nämnden ska regelbundet övervaka och utvärdera hur deltagarna uppnår förfarandekodernas mål och hur de bidrar till en korrekt tillämpning av denna förordning. AI-byrån och nämnden ska bedöma huruvida förfarandekoderna omfattar de skyldigheter som fastställs i artiklarna 53 och 55 samt de aspekter som förtecknas i punkt 2 i denna artikel, och ska regelbundet övervaka och utvärdera om målen i dem uppnås. De ska offentliggöra sin bedömning av förfarandekodernas lämplighet.

Kommissionen får genom en genomförandeakt godkänna en förfarandekod och ge den allmän giltighet inom unionen. Genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

7. AI-byrån får uppmana alla leverantörer av AI-modeller för allmänna ändamål att följa förfarandekoderna. För leverantörer av AI-modeller för allmänna ändamål som inte medför systemrisker får denna efterlevnad begränsas till de skyldigheter som föreskrivs i artikel 53, såvida de inte uttryckligen förklarar att de vill ansluta sig till den fullständiga koden.

8. AI-byrån ska, när så är lämpligt, också uppmuntra och underlätta översynen och anpassningen av förfarandekoderna, särskilt mot bakgrund av nya standarder. AI-byrån ska bistå vid bedömningen av tillgängliga standarder.

9. Förfarandekoder ska vara utarbetade senast den ... [nio månader efter dagen för denna förordnings ikraftträdande]. AI-byrån ska vidta nödvändiga åtgärder, bland annat genom att uppmana leverantörer i enlighet med punkt 7.

Om en förfarandekod inte kan färdigställas senast den ... [tolv månader efter dagen för ikraftträdande], eller om AI-byrån efter sin bedömning *enligt punkt 6 i denna artikel anser att den inte är lämplig, får kommissionen genom genomförandeakter fastställa gemensamma regler för genomförandet av de skyldigheter som föreskrivs i artiklarna 53 och 55, inbegripet de aspekter som anges i punkt 2 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.*

KAPITEL VI
ÅTGÄRDER TILL STÖD FÖR INNOVATION

Artikel 57

Regulatoriska sandlådor för AI

1. ***Medlemsstaterna ska säkerställa att deras behöriga myndigheter inrättar minst en regulatorisk sandlåda för AI på nationell nivå, som*** ska ***vara i drift senast den... [24 månader efter dagen för denna förordnings ikraftträdande]. Denna sandlåda får också inrättas tillsammans med de behöriga myndigheterna i en eller flera andra medlemsstater. Kommissionen får tillhandahålla tekniskt stöd, rådgivning och verktyg för inrättande och drift av regulatoriska sandlådor för AI.***

Skyldigheten enligt första stycket får också fullgöras genom deltagande i en befintlig sandlåda i den mån deltagandet ger en likvärdig nivå av nationell täckning för de deltagande medlemsstaterna.

2. Ytterligare regulatoriska sandlådor för AI får också inrättas på regional eller lokal nivå eller tillsammans med andra medlemsstaters behöriga myndigheter.

3. Europeiska datatillsynsmannen får också inrätta en regulatorisk sandlåda för AI för unionens institutioner, organ och byråer och får utöva de nationella behöriga myndigheternas roller och uppgifter i enlighet med detta kapitel.

4. Medlemsstaterna ska säkerställa att de behöriga myndigheter som avses i punkterna 1 och 2 anslår tillräckliga resurser för att uppfylla kraven i denna artikel, på ett ändamålsenligt sätt och i god tid. I lämpliga fall ska de nationella behöriga myndigheterna samarbeta med andra relevanta myndigheter, och de får tillåta deltagande av andra aktörer inom AI-ekosystemet. Denna artikel ska inte påverka andra regulatoriska sandlådor som inrättats enligt unionsrätten eller nationell rätt. Medlemsstaterna ska säkerställa lämpligt samarbete mellan de myndigheter som utövar tillsyn över dessa andra sandlådor och de nationella behöriga myndigheterna.

5. ***Regulatoriska sandlådor för AI som inrättats enligt punkt 1 ska tillhandahålla en kontrollerad miljö som främjar innovation och underlättar utveckling, träning, testning och validering av innovativa AI-system under en begränsad tid innan de släpps ut på marknaden eller tas i bruk i enlighet med en särskild sandlådeplan som de potentiella leverantörerna och den behöriga myndigheten kommer överens om. Sådana regulatoriska sandlådor får omfatta testning under verkliga förhållanden under tillsyn i sandlådan.***

6. ***De behöriga myndigheterna ska, beroende på vad som är lämpligt, tillhandahålla vägledning, tillsyn och stöd inom den regulatoriska sandlådan för AI i syfte att identifiera risker, särskilt när det gäller grundläggande rättigheter, hälsa och säkerhet, testning, riskreducerande åtgärder och deras effektivitet i förhållande till skyldigheterna och kraven i denna förordning samt, i förekommande fall, annan unionsrätt och medlemsstatsrätt som är föremål för tillsyn inom sandlådan.***

7. ***De behöriga myndigheterna ska ge leverantörer och potentiella leverantörer*** som använder den regulatoriska sandlådan för AI ***vägledning om rättsliga förväntningar och hur de krav och skyldigheter som fastställs i denna förordning ska uppfyllas.***

På begäran av leverantören eller den potentiella leverantören av AI-systemet ska den behöriga myndigheten tillhandahålla ett skriftligt bevis på den verksamhet som framgångsrikt utförts i sandlådan. Den behöriga myndigheten ska också tillhandahålla en slutrapport med uppgifter om den verksamhet som bedrivs i sandlådan och tillhörande resultat och läranderesultat. Leverantörer får använda sådan dokumentation för att visa att de uppfyller kraven i denna förordning genom förfarandet för bedömning av överensstämmelse eller relevant marknadskontroll. I detta avseende ska marknadskontrollmyndigheterna och de anmälda organen beakta slutrapporterna och de skriftliga bevis som tillhandahålls av den nationella behöriga myndigheten på ett positivt sätt, i syfte att påskynda förfaranden för bedömning av överensstämmelse i rimlig utsträckning.

8. Om inte annat följer av konfidentialitetsbestämmelserna i artikel 78 och med godkännande från leverantören eller den potentiella leverantören ska kommissionen och nämnden ha rätt att få tillgång till slutrapporterna och ska beakta dem, på lämpligt sätt, när de utför sina uppgifter enligt denna förordning. Om både leverantören eller den potentiella leverantören och den nationella behöriga myndigheten uttryckligen samtycker får slutrapporten göras allmänt tillgänglig via den enda informationsplattform som avses i denna artikel.

9. Inrättandet av regulatoriska sandlådor för AI ska syfta till att bidra till följande mål:

a) Förbättra rättssäkerheten för att uppnå efterlevnad av denna förordning eller, i förekommande fall, annan tillämplig unionsrätt och nationell rätt.

b) Stödja utbyte av bästa praxis genom samarbete med de myndigheter som deltar i den regulatoriska sandlådan för AI.

c) Främja innovation och konkurrenskraft och underlätta utvecklingen av ett AI-ekosystem.

d) Bidra till evidensbaserat regulatoriskt lärande.

e) Underlätta och påskynda tillgången till unionsmarknaden för AI-system, särskilt när de tillhandahålls av små och medelstora företag, inbegripet nystartade företag.

10. I den mån de innovativa AI-systemen inbegriper behandling av personuppgifter eller på annat sätt faller inom tillsynsområdet för andra nationella myndigheter eller behöriga myndigheter som tillhandahåller eller stöder åtkomst till data ska ***de nationella behöriga myndigheterna*** säkerställa att de nationella dataskyddsmyndigheterna och dessa andra nationella eller behöriga myndigheter är involverade i driften av den regulatoriska sandlådan för AI ***och i övervakningen av dessa aspekter så långt deras respektive uppgifter och befogenheter sträcker sig***.

11. De regulatoriska sandlådorna för AI ska inte påverka tillsynsbefogenheterna eller de korrigerande befogenheterna för de behöriga myndigheter ***som utövar tillsyn över sandlådorna, inbegripet på regional eller lokal nivå***. Alla betydande risker för hälsa och säkerhet och grundläggande rättigheter som upptäcks under utvecklingen och testningen av sådana ***AI-***system ska leda till ***adekvata*** begränsningsåtgärder. ***De nationella behöriga myndigheterna ska ha befogenhet att tillfälligt eller permanent avbryta testprocessen eller deltagandet*** i ***sandlådan om inga verkningsfulla begränsningsåtgärder är möjliga och ska informera AI-byrån om ett sådant beslut. De nationella behöriga myndigheterna ska utöva sina tillsynsbefogenheter inom ramen för relevant rätt, med användning av sitt utrymme för skönsmässig bedömning när de genomför rättsliga bestämmelser för ett specifikt sandlådeprojekt för AI, i syfte att stödja innovation inom AI i unionen.***

12. ***Leverantörer och potentiella leverantörer*** som deltar i den regulatoriska sandlådan för AI ska förbli ansvariga, enligt tillämplig unionsrätt och nationell rätt om ansvarsskyldighet, för ***skada*** som åsamkas tredje part till följd av de experiment som äger rum i sandlådan. ***Under förutsättning att de potentiella leverantörerna följer den särskilda planen och villkoren för deras deltagande samt i god tro följer de riktlinjer som den nationella behöriga myndigheten ger, ska myndigheterna dock inte ålägga några administrativa sanktionsavgifter för överträdelser av denna förordning. I den mån andra behöriga myndigheter med ansvar för annan unionsrätt och nationell rätt aktivt deltog i tillsynen av AI-systemet i sandlådan och tillhandahöll vägledning för efterlevnad ska inga administrativa sanktionsavgifter åläggas avseende den rätten.***

13. De regulatoriska sandlådorna för AI ska utformas och genomföras på ett sådant sätt att de i relevanta fall underlättar gränsöverskridande samarbete mellan de nationella behöriga myndigheterna.

14. De ***nationella*** behöriga myndigheterna ▌ ska samordna sin verksamhet och samarbeta inom ramen för ▌ nämnden. ▌

15. De nationella behöriga myndigheterna ska informera AI-byrån och nämnden om inrättandet av en sandlåda och får begära stöd och vägledning. AI-byrån ska göra en förteckning över planerade och befintliga AI-sandlådor allmänt tillgänglig och hålla den uppdaterad för att uppmuntra till mer interaktion i regulatoriska sandlådor för AI och gränsöverskridande samarbete.

16. De nationella behöriga myndigheterna ska lämna årliga rapporter till AI-byrån och nämnden, med början ett år efter att den regulatoriska sandlådan för AI har inrättats och därefter varje år fram till dess att den avslutas samt en slutrapport. Dessa rapporter ska innehålla information om framstegen och resultaten av genomförandet av dessa sandlådor, inbegripet bästa praxis, incidenter, tillvaratagna erfarenheter och rekommendationer om deras etablering och, i relevanta fall, om tillämpningen och en eventuell översyn av denna förordning, inbegripet dess delegerade akter och genomförandeakter, och om tillämpningen av annan unionsrätt som är föremål för tillsyn från de berörda myndigheterna inom sandlådan. De nationella behöriga myndigheterna ska göra dessa årliga rapporter eller sammanfattningar av dessa tillgängliga för allmänheten online. Kommissionen ska, när så är lämpligt, beakta årsrapporterna när den utför sina uppgifter enligt denna förordning.

17. *Kommissionen ska utveckla ett gemensamt och särskilt gränssnitt som innehåller all relevant information om regulatoriska sandlådor för AI för att göra det möjligt för berörda parter att interagera med regulatoriska sandlådor för AI och ta upp frågor med behöriga myndigheter samt söka icke-bindande vägledning om överensstämmelse för innovativa produkter, tjänster och affärsmodeller med inbäddad AI-teknik, i enlighet med artikel 62.1 c. Kommissionen ska proaktivt säkerställa samordning med nationella behöriga myndigheter, där så är relevant.*

Artikel 58

Närmare arrangemang och funktionssätt för regulatoriska sandlådor för AI

1. För att undvika fragmentering i hela unionen ska kommissionen anta genomförandeakter som specificerar de närmare arrangemangen för inrättande, utveckling, genomförande, drift och tillsyn av regulatoriska sandlådor för AI. Dessa genomförandeakter ska innehålla gemensamma principer i följande frågor:

a) Behörighets- och urvalskriterier för deltagande i den regulatoriska sandlådan för AI.

b) Förfarandet för tillämpning, deltagande, övervakning, utträde ur och avslutande av den regulatoriska sandlådan för AI, inbegripet sandlådeplanen och slutrapporten.

c) De villkor som gäller för deltagarna.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

2. De genomförandeakter som avses i punkt 1 ska säkerställa att

a) regulatoriska sandlådor för AI är öppna för alla potentiella leverantörer av ett AI-system som uppfyller behörighets- och urvalskriterier, som ska vara transparenta och rättvisa, och nationella behöriga myndigheter ska informera sökande om sitt beslut inom tre månader efter ansökan,

b) regulatoriska sandlådor för AI möjliggör bred och likvärdig tillgång och håller jämna steg med efterfrågan på deltagande; potentiella leverantörer får också lämna in ansökningar i partnerskap med användare och andra relevanta tredje parter,

c) närmare arrangemang och villkor för regulatoriska sandlådor för AI i möjligaste mån stöder de nationella behöriga myndigheternas flexibilitet att inrätta och driva sina regulatoriska sandlådor för AI,

d) tillgången till regulatoriska sandlådor för AI är kostnadsfri för små och medelstora företag, inbegripet nystartade företag, utan att det påverkar exceptionella kostnader som nationella behöriga myndigheter får återkräva på ett rättvist och proportionellt sätt,

e) de, genom läranderesultaten från de regulatoriska sandlådorna för AI, gör det lättare för potentiella leverantörer att fullgöra skyldigheterna avseende bedömning av överensstämmelse enligt denna förordning och den frivilliga tillämpningen av de uppförandekoder som avses i artikel 95,

f) regulatoriska sandlådor för AI underlättar deltagandet av andra relevanta aktörer inom AI-ekosystemet, såsom anmälda organ och standardiseringsorganisationer, små och medelstora företag, nystartade företag och andra företag, innovatörer, test- och experimentanläggningar, forsknings- och experimentlaboratorier och europeiska digitala innovationsknutpunkter, kompetenscentrum samt enskilda forskare, för att möjliggöra och underlätta samarbete med den offentliga och privata sektorn,

g) förfaranden, processer och administrativa krav för ansökan och urval till, deltagande i och utträde ur den regulatoriska sandlådan för AI ska vara enkla, lättbegripliga och tydligt kommunicerade för att underlätta deltagandet av små och medelstora företag, inbegripet nystartade företag, med begränsad rättslig och administrativ kapacitet och strömlinjeformas i hela unionen i syfte att undvika fragmentering, och att deltagande i en regulatorisk sandlåda för AI som inrättats av en medlemsstat eller av Europeiska datatillsynsmannen erkänns ömsesidigt och enhetligt och har samma rättsliga verkan i hela unionen,

h) deltagandet i den regulatoriska sandlådan för AI är begränsat till en period som är lämplig med tanke på projektets komplexitet och omfattning, vilken får förlängas av den nationella behöriga myndigheten,

i) de regulatoriska sandlådorna för AI underlättar utvecklingen av verktyg och infrastruktur för testning, riktmärkning, bedömning och förklaring av de aspekter av AI-systemen som är relevanta för regulatoriskt lärande, såsom noggrannhet, robusthet och cybersäkerhet samt minimering av riskerna för de grundläggande rättigheterna och samhället i stort.

3. Potentiella leverantörer i regulatoriska sandlådor för AI, särskilt små och medelstora företag och nystartade företag, ska, när så är relevant, hänvisas till tjänster före ibruktagandet, såsom vägledning om genomförandet av denna förordning, andra mervärdestjänster såsom hjälp med standardiseringsdokument och certifiering, test- och experimentanläggningar, europeiska digitala innovationsknutpunkter och kompetenscentrum.

4. När nationella behöriga myndigheter överväger att godkänna testning under verkliga förhållanden som står under tillsyn inom ramen för en regulatorisk sandlåda för AI som ska inrättas enligt denna artikel, ska de särskilt komma överens med deltagarna om villkoren för sådan testning och i synnerhet om lämpliga garantier i syfte att skydda grundläggande rättigheter, hälsa och säkerhet. I lämpliga fall ska de samarbeta med andra nationella behöriga myndigheter i syfte att säkerställa enhetlig praxis i hela unionen.

Artikel 59

Ytterligare behandling av personuppgifter för utveckling av vissa AI-system i allmänhetens intresse i den regulatoriska sandlådan för AI

1. Personuppgifter som lagligen samlats in för andra ändamål ***får*** behandlas i en regulatorisk sandlåda för AI ***enbart*** i syfte att utveckla***, träna*** och testa vissa ▌ AI-system i sandlådan ***om samtliga*** följande villkor ***är uppfyllda***:

   a) ▌ AI-systemen ska utvecklas för att ett väsentligt allmänintresse ska skyddas ***av en offentlig myndighet eller annan fysisk eller juridisk person*** på ett eller flera av följande områden:

      i) Allmän säkerhet och folkhälsa, inbegripet ***upptäckt, diagnostisering,*** förebyggande, bekämpning och behandling av sjukdomar ***och förbättring av hälso- och sjukvårdssystemen***.

      ii) En hög nivå av skydd och förbättring av miljöns kvalitet***, skydd av den biologiska mångfalden, skydd mot föroreningar, åtgärder för grön omställning samt begränsning av och anpassning till klimatförändringar***.

iii) Energihållbarhet.

iv) Säkerhet och resiliens när det gäller transportsystem och mobilitet, kritisk infrastruktur och nätverk.

v) Den offentliga förvaltningens och de offentliga tjänsternas effektivitet och kvalitet.

b) De data som behandlas är nödvändiga för att uppfylla ett eller flera av de krav som avses i kapitel III avsnitt 2 i fall där dessa krav inte kan uppfyllas effektivt genom behandling av anonymiserade eller syntetiska data eller andra icke-personuppgifter.

c) Det finns effektiva övervakningsmekanismer för att fastställa om experimenten i sandlådan kan medföra höga risker för de registrerades ***rättigheter och friheter, enligt artikel 35 i förordning (EU) 2016/679 och artikel 39 i förordning (EU) 2018/1725,*** samt en svarsmekanism för att snabbt begränsa dessa risker och, vid behov, stoppa behandlingen.

d) Alla personuppgifter som ska behandlas inom ramen för sandlådan befinner sig i en funktionellt separat, isolerad och skyddad databehandlingsmiljö under den ***potentiella leverantörens*** kontroll, och endast behöriga personer har tillgång till ***dessa*** uppgifter.

e) ***Leverantörerna kan endast dela vidare de ursprungligen insamlade uppgifterna i enlighet med unionens dataskyddslagstiftning.*** Personuppgifter ***som skapats i sandlådan får inte delas utanför sandlådan.***

f) Behandling av personuppgifter i samband med sandlådan ska varken leda till åtgärder eller beslut som påverkar de registrerade ***eller påverka tillämpningen av deras rättigheter enligt unionsrätten om skydd av personuppgifter***.

g) Alla personuppgifter som behandlas inom ramen för sandlådan ska ***skyddas genom lämpliga tekniska och organisatoriska åtgärder och*** raderas när deltagandet i sandlådan har avslutats eller personuppgifternas lagringstid har löpt ut.

h) Loggarna över behandlingen av personuppgifter inom ramen för sandlådan ska bevaras under den tid som deltagandet i sandlådan varar***, om inte annat föreskrivs i*** unionsrätten eller ***nationell rätt***,

i) En fullständig och detaljerad beskrivning av processen och motiveringen för träning, testning och validering av AI-systemet bevaras tillsammans med testresultaten som en del av den tekniska dokumentation som avses i bilaga IV.

j) En kort sammanfattning av AI-projektet som utvecklats i sandlådan, dess mål och förväntade resultat offentliggörs på den behöriga myndighetens webbplats. ***Denna skyldighet ska inte omfatta känsliga operativa uppgifter som rör brottsbekämpande myndigheters, gränskontrollmyndigheters, invandringsmyndigheters eller asylmyndigheters verksamhet.***

2. I syfte att förebygga, förhindra, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder, inbegripet att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, under brottsbekämpande myndigheters överinseende och ansvar, ska behandlingen av personuppgifter i regulatoriska sandlådor för AI baseras på specifik unionsrätt eller nationell rätt och omfattas av samma kumulativa villkor som dem som avses i punkt 1.

3. Punkt 1 ska inte påverka tillämpningen av unionsrätt eller nationell rätt som utesluter behandling av personuppgifter för andra ändamål än dem som uttryckligen anges i den rätten ***samt av unionsrätt eller nationell rätt om grunden för behandling av personuppgifter som är nödvändig för att utveckla, testa eller träna innovativa AI-system, eller av någon annan rättslig grund, i enlighet med unionsrätten om skydd av personuppgifter***.

Artikel 60

Testning av AI-system med hög risk under verkliga förhållanden utanför regulatoriska sandlådor för AI

1. Testning av AI-system med hög risk under verkliga förhållanden utanför regulatoriska sandlådor för AI får utföras av leverantörer eller potentiella leverantörer av AI-system med hög risk som förtecknas i bilaga III, i enlighet med denna artikel och den plan för testning under verkliga förhållanden som avses i denna artikel, utan att det påverkar förbuden enligt artikel 5.

De närmare inslagen i planen för testning under verkliga förhållanden ska specificeras i genomförandeakter som ska antas av kommissionen i enlighet med det granskningsförfarande som avses i artikel 98.2.

Denna bestämmelse ska inte påverka tillämpningen av unionsrätten eller nationell rätt om testning under verkliga förhållanden av AI-system med hög risk som är relaterade till produkter som omfattas av den lagstiftning som förtecknas i bilaga I.

2. Leverantörer eller potentiella leverantörer får på egen hand eller i partnerskap med en eller flera potentiella spridare utföra testning under verkliga förhållanden av AI-system med hög risk som avses i bilaga III när som helst innan AI-systemet släpps ut på marknaden eller tas i bruk.

3. Testning av AI-system med hög risk under verkliga förhållanden enligt denna artikel ska inte påverka etisk granskning som krävs enligt nationell rätt eller unionsrätten.

4. Leverantörer eller potentiella leverantörer får utföra testningen under verkliga förhållanden endast om samtliga följande villkor är uppfyllda:

a) Leverantören eller den potentiella leverantören har utarbetat en plan för testning under verkliga förhållanden och lämnat in den till marknadskontrollmyndigheten i den medlemsstat där testningen under verkliga förhållanden ska utföras.

b) Marknadskontrollmyndigheten i den medlemsstat där testningen under verkliga förhållanden ska utföras har godkänt testningen under verkliga förhållanden och planen för testning under verkliga förhållanden. Om marknadskontrollmyndigheten inte har lämna något svar inom 30 dagar ska testningen under verkliga förhållanden och planen för testning under verkliga förhållanden betraktas som godkänd. Om det enligt nationell rätt inte föreskrivs något tyst godkännande, ska testningen under verkliga förhållanden fortfarande förutsätta ett tillstånd.

c) Leverantören eller den potentiella leverantören, med undantag för leverantörer eller potentiella leverantörer av AI-system med hög risk som avses i punkterna 1, 6 och 7 i bilaga III på områdena brottsbekämpning, migration, asyl och gränskontrollförvaltning samt AI-system med hög risk som avses i punkt 2 i bilaga III, har registrerat testning under verkliga förhållanden i den icke-offentliga delen av den EU-databas som avses i artikel 71.3 med ett enda unionsomfattande identifieringsnummer och den information som anges i bilaga IX.

d) Den leverantör eller potentiella leverantör som utför testningen under verkliga förhållanden är etablerad i unionen eller har utsett ett juridiskt ombud som är etablerat i unionen.

e) Uppgifter som samlats in och behandlats för testning under verkliga förhållanden ska överföras till tredjeländer endast om lämpliga och tillämpliga skyddsåtgärder enligt unionsrätten vidtas.

f) Testningen under verkliga förhållanden varar inte längre än vad som är nödvändigt för att uppnå dess mål och under inga omständigheter längre än sex månader, med möjlighet till förlängning med ytterligare sex månader om leverantören gör en förhandsanmälan till marknadskontrollmyndigheten som ska åtföljas av en förklaring av behovet av en sådan förlängning.

g) Försökspersoner i testningen under verkliga förhållanden som är ***sårbara personer på grund av ålder eller fysisk eller psykisk funktionsnedsättning skyddas på lämpligt sätt.***

h) Om en leverantör eller potentiell leverantör organiserar testningen under verkliga förhållanden i samarbete med en eller flera spridare eller potentiella spridare, har dessa informerats om alla aspekter av testningen som är relevanta för deras beslut att delta och fått den relevanta bruksanvisningen för det AI-system som avses i artikel 13; leverantören eller den potentiella leverantören och den potentiella spridaren ska ingå ett avtal som anger deras roller och ansvar i syfte att säkerställa överensstämmelse med bestämmelserna om testning under verkliga förhållanden enligt denna förordning och övrig tillämplig unionsrätt och nationell rätt.

i) Försökspersonerna i testningen under verkliga förhållanden har gett sitt informerade samtycke i enlighet med artikel 61, eller, när det gäller brottsbekämpning, om en begäran om informerat samtycke skulle hindra AI-systemet att testas, själva testningen och resultatet av testningen under verkliga förhållanden har inte någon negativ inverkan på försökspersonerna, vars personuppgifter ska raderas när testningen har utförts.

j) Testningen under verkliga förhållanden övervakas effektivt av leverantören eller den potentiella leverantören och av spridarna eller de potentiella spridarna genom personer som har lämpliga kvalifikationer inom det berörda området och som har nödvändig kapacitet, utbildning och auktoritet för att utföra sina uppgifter.

k) AI-systemets förutsägelser, rekommendationer eller beslut kan effektivt upphävas eller ignoreras.

5. Försökspersoner inom testningen under verkliga förhållanden, eller deras lagligen utsedda företrädare, beroende på vad som är lämpligt, får, utan att detta medför nackdelar och utan att behöva lämna någon motivering, när som helst avsluta sitt deltagande i testningen genom att dra tillbaka sitt informerade samtycke och får begära omedelbar och permanent radering av sina personuppgifter. Tillbakadragandet av det informerade samtycket ska inte påverka lagligheten eller giltigheten för den verksamhet som redan utförts.

6. I enlighet med artikel 75 ska medlemsstaterna ge sina marknadskontrollmyndigheter befogenhet att kräva att leverantörer och potentiella leverantörer tillhandahåller information, att utföra oanmälda inspektioner på distans eller på plats och att utföra kontroller av utvecklingen av testningen under verkliga förhållanden och tillhörande produkter. Marknadskontrollmyndigheterna ska använda dessa befogenheter för att säkerställa en säker utveckling av testning under verkliga förhållanden.

7. Alla allvarliga incidenter som identifieras under testningen under verkliga förhållanden ska rapporteras till den nationella marknadskontrollmyndigheten i enlighet med artikel 73. Leverantören eller den potentiella leverantören ska vidta omedelbara riskbegränsningsåtgärder eller, om så inte sker, tillfälligt avbryta testningen under verkliga förhållanden tills sådan riskreducering äger rum eller i annat fall avsluta den. Leverantören eller den potentiella leverantören ska fastställa ett förfarande för snabb återkallelse av AI-systemet när testningen under verkliga förhållanden avslutas på detta sätt.

8. Leverantörer eller potentiella leverantörer ska underrätta den nationella marknadskontrollmyndigheten i den medlemsstat där testningen under verkliga förhållanden ska utföras om det tillfälliga avbrottet i eller avslutandet av testningen under verkliga förhållanden och om de slutliga resultaten.

9. Leverantören och den potentiella leverantören ska vara ansvariga enligt unionens och medlemsstaternas tillämpliga lagstiftning om ansvar för eventuella skador som orsakas under deras deltagande i testningen under verkliga förhållanden.

Artikel 61

Informerat samtycke till deltagande i testning under verkliga förhållanden utanför regulatoriska sandlådor för AI

1. För testning under verkliga förhållanden enligt artikel 60 ska frivilligt lämnat informerat samtycke erhållas från försökspersonerna innan de deltar i sådan testning och efter att de vederbörligen har informerats med koncis, tydlig, relevant och begriplig information om

a) vilken karaktär och vilka mål som testningen under verkliga förhållanden har och de eventuella olägenheter som kan vara förknippade med att delta,

b) de förhållanden under vilka testningen under verkliga förhållanden ska utföras, inbegripet den förväntade varaktigheten för försökspersonens eller försökspersonernas deltagande,

c) sina rättigheter och garantierna avseende deras deltagandet, särskilt sin rätt att vägra att delta och att när som helst avsluta sitt deltagande i testningen under verkliga förhållanden utan negativa följder och utan att behöva motivera sitt beslut,

d) formerna för begäran om upphävande eller ignorerande av AI-systemets förutsägelser, rekommendationer eller beslut,

e) det enda unionsomfattande identifieringsnumret för testningen under verkliga förhållanden i enlighet med artikel 60.4 c ***och kontaktuppgifter för leverantören eller dennes juridiska ombud från vilka ytterligare information kan erhållas.***

2. Det informerade samtycket ska dateras och dokumenteras och en kopia ska ges till försökspersonerna i testningen eller till deras juridiska ombud.

Artikel 62

Åtgärder för ▌ *leverantörer och* ***spridare, särskilt små och medelstora företag, inbegripet nystartade företag***

1. Medlemsstaterna ska vidta följande åtgärder:

a) Ge små och medelstora företag, inbegripet nystartade företag***, som har ett säte eller en filial i unionen*** prioriterad åtkomst till de regulatoriska sandlådorna för AI, i den mån de uppfyller behörighetskraven ***och urvalskriterierna***. ***Den prioriterade åtkomsten ska inte hindra andra små och medelstora företag, inbegripet uppstartsföretag, än dem som avses i första stycket, att ha tillgång till den regulatoriska sandlådan för AI, förutsatt att de också uppfyller behörighetskraven och urvalskriterierna***.

b) Anordna särskilda medvetandehöjande åtgärder ***och utbildning om*** tillämpningen av denna förordning anpassat till behoven hos ***små och medelstora företag, inbegripet nystartade företag, och, i lämpliga fall, lokala offentliga myndigheter***.

c) ***Använda befintliga särskilda kanaler och,*** i lämpliga fall, upprätta ***nya sådana*** för kommunikation med ***små och medelstora företag, inbegripet nystartade företag, användare, andra innovatörer och, om lämpligt, lokala offentliga myndigheter***, för att ge ***råd*** och svara på frågor om genomförandet av denna förordning***, inbegripet när det gäller deltagande i regulatoriska sandlådor för AI***.

d) Underlätta små och medelstora företags och andra berörda parters deltagande i processen för standardiseringsutveckling.

2. De särskilda intressen och behov som ***små och medelstora företag, inbegripet nystartade företag,*** har som leverantörer ska beaktas när avgifterna för bedömning av överensstämmelse enligt artikel 43 fastställs, och avgifterna ska minskas i proportion till deras storlek, ***marknadsstorlek och andra relevanta indikatorer***.

3. AI-byrån ska vidta följande åtgärder:

a) Tillhandahålla standardiserade mallar för områden som omfattas av denna förordning, i enlighet med nämndens anvisningar i dess motiverade begäran.

b) Utveckla och upprätthålla en enda informationsplattform som ger information som är lätt att använda om denna förordning till alla operatörer i hela unionen.

c) Anordna lämpliga kommunikationskampanjer för att öka medvetenheten om de skyldigheter som följer av denna förordning,

d) Utvärdera och främja konvergens av bästa praxis i förfaranden för offentlig upphandling när det gäller AI-system.

Artikel 63

Undantag för särskilda operatörer

1. Mikroföretag i den mening som avses i rekommendation 2003/361/EG får på ett förenklat sätt efterleva vissa delar av det kvalitetsstyrningssystem som krävs enligt artikel 17 i denna förordning, förutsatt att de inte har partnerföretag eller anknutna företag i den mening som avses i den rekommendationen. För detta ändamål ska kommissionen utarbeta riktlinjer för de delar av kvalitetsstyrningssystemet som får efterlevas på ett förenklat sätt med beaktande av mikroföretagens behov, utan att det påverkar skyddsnivån eller behovet av efterlevnad av kraven med avseende på AI-system med hög risk.

2. Punkt 1 ***i denna artikel ska inte tolkas som att dessa operatörer undantas från att uppfylla andra krav eller fullgöra andra skyldigheter som fastställs i denna förordning, inbegripet dem som fastställs i artiklarna 9, 10, 11, 12, 13, 14, 15, 72 och 73.***

KAPITEL VII
STYRNING

Avsnitt 1

Styrning på unionsnivå

Artikel 64
AI-byrån

1. Kommissionen ska utveckla unionens sakkunskap och kapacitet på AI-området genom AI-byrån.

2. Medlemsstaterna ska underlätta de uppgifter som anförtros AI-byrån, i enlighet med vad som återspeglas i denna förordning.

Artikel 65

Inrättande av och strukturen för den europeiska nämnden för artificiell intelligens

1. En europeisk nämnd för artificiell intelligens (*nämnden*) inrättas härmed.

2. Nämnden ska bestå av en företrädare per medlemsstat. Europeiska datatillsynsmannen ska delta som observatör. Även AI-byrån ska närvara vid nämndens möten, utan att delta i omröstningarna. Andra myndigheter, organ eller experter på nationell nivå och unionsnivå får bjudas in till mötena av nämnden från fall till fall, om de frågor som diskuteras är relevanta för dem.

3. Varje företrädare ska utses av sin medlemsstat för en period på tre år som får förnyas en gång.

4. Medlemsstaterna ska säkerställa att deras företrädare i nämnden

a) har relevant behörighet och relevanta befogenheter i sin medlemsstat för att aktivt bidra till fullgörandet av nämndens uppgifter enligt artikel 66,

b) utses till gemensam kontaktpunkt gentemot nämnden och när så är lämpligt, med beaktande av medlemsstaternas behov, till gemensam kontaktpunkt för de berörda parterna,

c) har befogenhet att underlätta enhetlighet och samordning mellan nationella behöriga myndigheter i sina medlemsstater när det gäller genomförandet av denna förordning, bland annat genom insamling av relevanta uppgifter och relevant information för att de ska kunna fullgöra sina uppgifter i nämnden.

5. Medlemsstaternas utsedda företrädare ska anta nämndens arbetsordning med två tredjedels majoritet. Arbetsordningen ska särskilt föreskriva förfaranden för urvalsprocessen, mandatets varaktighet och specifikationer för ordförandens uppgifter, närmare omröstningsregler och organisationen av nämndens och dess arbetsgruppers verksamhet.

6. Nämnden ska inrätta två ständiga arbetsgrupper som ska tillhandahålla en plattform för samarbete och utbyte mellan marknadskontrollmyndigheter och för underrättande av myndigheter i frågor som rör marknadskontroll och anmälda organ.

Den ständiga arbetsgruppen för marknadskontroll bör fungera som grupp för administrativt samarbete (Adco-grupp) för denna förordning i den mening som avses i artikel 30 i förordning (EU) 2019/1020.

Nämnden får inrätta andra ständiga eller tillfälliga undergrupper när så är lämpligt i syfte att granska specifika frågor. När så är lämpligt får företrädare för det rådgivande forum som avses i artikel 67 bjudas in till sådana arbetsgrupper eller till särskilda möten i dessa arbetsgrupper som observatörer.

7. Nämnden ska vara organiserad och fungera på ett sådant sätt att objektiviteten och opartiskheten i dess verksamhet skyddas.

8. En av företrädarna för medlemsstaterna ska vara ordförande i nämnden. AI-byrån ska bistå nämnden med ett sekretariat, sammankalla till möten på begäran av ordföranden och förbereda dagordningen i enlighet med nämndens uppdrag enligt denna förordning och nämndens arbetsordning.

Artikel 66

Nämndens uppgifter

Nämnden ska ge råd till och bistå kommissionen och medlemsstaterna för att underlätta en konsekvent och effektiv tillämpning av denna förordning. För detta ändamål får nämnden särskilt

a) ***bidra till samordningen mellan de nationella behöriga myndigheter som ansvarar för tillämpningen av denna förordning och, i samarbete med de berörda marknadskontrollmyndigheterna och med dessas samtycke, stödja marknadskontrollmyndigheternas gemensamma aktiviteter, som avses i artikel*** 74.11,

b) ***samla in och utbyta teknisk och*** regleringsmässig ***sakkunskap och bästa praxis bland medlemsstaterna***,

c) ge råd om genomförandet av denna förordning, särskilt när det gäller efterlevnaden av reglerna om AI-modeller för allmänna ändamål,

d) bidra till harmoniseringen av administrativ praxis i medlemsstaterna, inbegripet när det gäller det undantag från de förfaranden för bedömning av överensstämmelse som avses i artikel 46, de regulatoriska sandlådornas funktion och testning under verkliga förhållanden som avses i artiklarna 57, 59 och 60,

e) på begäran av kommissionen eller på eget initiativ utfärda rekommendationer ***och*** skriftliga ***yttranden om alla relevanta*** frågor som rör genomförandet av denna förordning ***och dess konsekventa och effektiva tillämpning, inbegripet***

i) om utarbetande och tillämpning av uppförandekoder och förfarandekoder i enlighet med denna förordning samt av kommissionens riktlinjer,

ii) utvärderingen och översynen av denna förordning i enlighet med artikel 112, inbegripet när det gäller de rapporter om allvarliga incidenter som avses i artikel 73, och funktionen för den databas som avses i artikel 71, utarbetandet av delegerade akter eller genomförandeakter, och vad gäller eventuella anpassningar av denna förordning till de rättsakter som förtecknas i bilaga I,

iii) om tekniska specifikationer eller befintliga standarder avseende de krav som anges i kapitel III avsnitt 2,

iv) om användning av harmoniserade standarder eller gemensamma specifikationer som avses i artiklarna 40 och 41,

v) trender, såsom europeisk global konkurrenskraft inom AI, användningen av AI i unionen och utvecklingen av digitala färdigheter,

vi) trender för ***AI-värdekedjors föränderliga typologi, särskilt när det gäller de därav följande konsekvenserna vad gäller ansvarsskyldighet,***

vii) om det potentiella behovet av att ändra bilaga III i enlighet med artikel 7 och om det potentiella behovet av en eventuell översyn av artikel 5 i enlighet med artikel 112, med beaktande av relevanta tillgängliga bevis och den senaste teknikutvecklingen,

f) stödja kommissionen med att främja AI-kunskap, allmänhetens medvetenhet om och förståelsen av fördelar, risker, skyddsåtgärder och rättigheter och skyldigheter i samband med användningen av AI-system,

g) underlätta utvecklingen av gemensamma kriterier och en gemensam förståelse bland marknadsaktörer och behöriga myndigheter om de relevanta begrepp som anges i denna förordning, inbegripet genom att bidra till utvecklingen av riktmärken,

h) vid behov samarbeta med andra av unionens institutioner, organ, och byråer och med unionens relevanta expertgrupper och nätverk, särskilt på områdena produktsäkerhet, cybersäkerhet, konkurrenskraft, digitala tjänster och medietjänster, finansiella tjänster, konsumentskydd, dataskydd och skydd av grundläggande rättigheter,

i) bidra till ett effektivt samarbete med behöriga myndigheter i tredjeländer och med internationella organisationer,

j) bistå nationella behöriga myndigheter och kommissionen i utvecklingen av den organisatoriska och tekniska expertis som krävs för genomförandet av denna förordning, bland annat genom att bidra till bedömningen av utbildningsbehoven för den personal från medlemsstater som deltar i genomförandet av denna förordning.

k) bistå AI-byrån i stödet till nationella behöriga myndigheter vid inrättandet och utvecklingen av regulatoriska sandlådor, och underlätta samarbete och informationsutbyte mellan regulatoriska sandlådor,

l) bidra till och ge relevanta råd om utarbetandet av vägledande handlingar,

m) ge kommissionen råd i internationella AI-frågor,

n) avge yttranden till kommissionen om kvalificerade varningar avseende AI-modeller för allmänna ändamål,

o) ta emot yttranden från medlemsstaterna om kvalificerade varningar om AI-modeller för allmänna ändamål och om nationella erfarenheter och nationell praxis när det gäller övervakning och tillsyn av AI-system, särskilt system som integrerar AI-modellerna för allmänna ändamål.

Artikel 67

Rådgivande forum

1. Ett rådgivande forum ska inrättas för att tillhandahålla teknisk expertis och ge råd till nämnden och kommissionen och bidra till deras uppgifter enligt denna förordning.

2. Medlemmarna i det rådgivande forumet ska representera ett balanserat urval av berörda parter, däribland branschen, nystartade företag, små och medelstora företag, det civila samhället, och den akademiska världen. Sammansättningen av det rådgivande forumet ska vara balanserad med avseende på kommersiella och icke-kommersiella intressen samt, inom kategorin kommersiella intressen, med avseende på små och medelstora företag och andra företag.

3. Kommissionen ska utse medlemmarna i det rådgivande forumet i enlighet med kriterierna i punkt 2 bland berörda parter med erkänd sakkunskap på AI-området.

4. Mandatperioden för medlemmarna i det rådgivande forumet ska vara två år, som får förlängas med högst fyra år.

5. Europeiska unionens byrå för grundläggande rättigheter, Europeiska unionens cybersäkerhetsbyrå (Enisa), Europeiska standardiseringskommittén (CEN), Europeiska kommittén för elektroteknisk standardisering (Cenelec) och Europeiska institutet för telekommunikationsstandarder (Etsi) ska vara ständiga medlemmar i det rådgivande forumet.

6. Det rådgivande forumet ska själv utarbeta sin arbetsordning. Den ska välja två medordförande bland sina medlemmar i enlighet med kriterierna i punkt 2. Medordförandenas mandatperiod ska vara två år och får förlängas en gång.

7. Det rådgivande forumet ska hålla möten minst två gånger per år. Det rådgivande forumet får bjuda in experter och andra berörda parter till sina möten.

8. Det rådgivande forumet får utarbeta yttranden, rekommendationer och skriftliga bidrag på begäran av nämnden eller kommissionen.

9. Det rådgivande forumet får inrätta permanenta eller tillfälliga arbetsgrupper enligt vad som är lämpligt för att utreda specifika frågor med avseende på målen för denna förordning.

10. Det rådgivande forumet ska utarbeta en årsrapport om sin verksamhet. Den rapporten ska göras allmänt tillgänglig.

Artikel 68

Vetenskaplig panel av oberoende experter

1. Kommissionen ska genom en genomförandeakt fastställa bestämmelser om inrättandet av en vetenskaplig panel av oberoende experter (den vetenskapliga panelen) som ska stödja verksamheten för efterlevnadskontroll enligt denna förordning. Genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

2. Den vetenskapliga panelen ska bestå av experter som valts ut av kommissionen på grundval av aktuell vetenskaplig eller teknisk expertis på AI-området och som är nödvändiga för de uppgifter som anges i punkt 3, och de ska kunna visa att de uppfyller samtliga följande villkor:

a) Särskild sakkunskap och kompetens samt vetenskaplig eller teknisk expertis på AI-området.

b) Oberoende ställning i förhållande till leverantörer av AI-system eller AI-system eller AI-modeller för allmänna ändamål.

c) Förmåga att bedriva verksamhet aktsamt, korrekt och objektivt. Kommissionen ska i samråd med nämnden fastställa antalet experter i panelen i enlighet med vad som krävs och säkerställa en rättvis könsfördelning och geografisk representation.

3. Den vetenskapliga panelen ska ge råd till och stödja AI-byrån, särskilt när det gäller följande uppgifter:

a) Stödja genomförandet och kontrollen av efterlevnaden av denna förordning vad gäller AI-modeller och AI-system för allmänna ändamål, särskilt genom att

i) varna AI-byrån för eventuella systemrisker på unionsnivå för AI-modeller för allmänna ändamål, i enlighet med artikel 90,

ii) bidra till utvecklingen av verktyg och metoder för utvärdering av kapaciteten hos AI-modeller och AI-system för allmänna ändamål, bland annat genom riktmärken,

iii) ge råd om klassificeringen av AI-modeller för allmänna ändamål med systemrisk,

iv) ge råd om klassificeringen av olika AI-modeller för allmänna ändamål och AI-system för allmänna ändamål,

v) bidra till utvecklingen av verktyg och mallar.

b) På begäran av marknadskontrollmyndigheterna stödja deras arbete.

c) Stödja gränsöverskridande marknadskontrollsverksamhet enligt artikel 74.11, utan att det påverkar marknadskontrollmyndigheternas befogenheter.

d) Stödja AI-byrån när den utför sina uppgifter inom ramen för skyddsklausulen enligt artikel 81.

4. Experterna i den vetenskapliga panelen ska utföra sina uppgifter opartiskt och objektivt och säkerställa att den information och de uppgifter som de erhåller vid utförandet av sina uppgifter och sin verksamhet behandlas konfidentiellt. De får varken begära eller ta emot instruktioner från någon när de utövar sina uppgifter enligt punkt 3. Varje expert ska avge en intresseförklaring, som ska göras allmänt tillgänglig. AI-byrån ska fastställa system och förfaranden för att aktivt hantera och förebygga potentiella intressekonflikter.

5. Den genomförandeakt som avses i punkt 1 ska innehålla bestämmelser om villkor, förfaranden och närmare arrangemang för att den vetenskapliga panelen och dess medlemmar ska utfärda varningar och begära bistånd från AI-byrån för utförandet av den vetenskapliga panelens uppgifter.

Artikel 69

Medlemsstaternas tillgång till poolen av experter

1. *Medlemsstaterna får anlita experter i den vetenskapliga panelen för att stödja deras verksamhet för efterlevnadskontroll enligt denna förordning.*

2. *Medlemsstaterna får åläggas att betala avgifter för experternas rådgivning och stöd. Avgifternas struktur och nivå samt de ersättningsgilla kostnadernas omfattning och struktur ska anges i den genomförandeakt som avses i artikel 68.1, med beaktande av målen att få till stånd ett korrekt genomförande av denna förordning, kostnadseffektivitet och behovet av att säkerställa att alla medlemsstater har faktisk tillgång till experter.*

3. *Kommissionen ska vid behov underlätta för medlemsstaterna att i tid få tillgång till experterna och ska säkerställa att kombinationen av den stödverksamhet som utförs av unionens stödstrukturer för AI-testning i enlighet med artikel* 84 *och experter i enlighet med denna artikel organiseras effektivt och tillför bästa möjliga mervärde.*

Avsnitt 2
Nationella behöriga myndigheter

Artikel 70

Utseende av nationella behöriga myndigheter ***och gemensam kontaktpunkt***

1. Varje medlemsstat ska ***vid tillämpning av denna förordning*** som nationella behöriga myndigheter inrätta eller till sådana utse ***inrätta eller*** utse ***minst en anmälande myndighet och minst en marknadskontroll***myndighet. ***Dessa nationella behöriga myndigheter ska utöva sina befogenheter på ett oberoende, objektivt och opartiskt sätt för att säkerställa objektiviteten i sina aktiviteter och uppgifter och för att säkerställa tillämpningen och genomförandet av denna förordning***. ***Ledamöterna i dessa myndigheter ska avhålla sig från varje handling som är oförenlig med deras uppdrag. Förutsatt att dessa principer respekteras får sådana aktiviteter och uppgifter utföras av en eller flera utsedda myndigheter, i enlighet med medlemsstatens organisatoriska behov***.

2. Medlemsstaterna ska ***meddela*** kommissionen ***identiteten på de anmälande myndigheterna och marknadskontrollmyndigheterna och dessa myndigheters uppgifter samt eventuella senare ändringar av dessa***. ***Medlemsstaterna ska göra information om hur behöriga myndigheter och gemensamma kontaktpunkter kan kontaktas genom elektroniska kommunikationsmedel allmänt tillgänglig senast den... [12 månader från och med dagen för denna förordnings ikraftträdande]. Medlemsstaterna ska utse en marknadskontrollmyndighet som ska fungera som gemensam kontaktpunkt för denna förordning och underrätta kommissionen om den gemensamma kontaktpunktens identitet. Kommissionen ska göra en förteckning över gemensamma kontaktpunkter allmänt tillgänglig.***

3. Medlemsstaterna ska säkerställa att ***deras*** nationella behöriga myndigheter har tillräckliga ***tekniska*** och ekonomiska resurser samt personalresurser***, och infrastruktur*** för att kunna fullgöra sina uppgifter ***på ett ändamålsenligt sätt*** enligt denna förordning. I synnerhet ska de nationella behöriga ***myndigheterna*** ha ett tillräckligt antal anställda till ständigt förfogande, vars kompetens och sakkunskap ska inbegripa en ingående förståelse av AI-teknik, data och databehandling, ***skydd av personuppgifter, cybersäkerhet,*** grundläggande rättigheter, hälso- och säkerhetsrisker och kunskap om befintliga standarder och rättsliga krav. ***Medlemsstaterna ska varje år bedöma och, vid behov, uppdatera de kompetens- och resurskrav som avses i denna punkt.***

4. De nationella behöriga myndigheterna ska vidta tillräckliga cybersäkerhetsåtgärder.

5. De nationella tillsynsmyndigheterna ska när de utför sina uppgifter agera i enlighet med de konfidentialitetskrav som anges i artikel 78.

6. ***Senast den... [ett år från och med dagen för denna förordnings ikraftträdande] och därefter vartannat år*** ska medlemsstaterna rapportera till ▌ kommissionen om statusen för de nationella behöriga myndigheternas ekonomiska resurser och personalresurser, med en bedömning av deras tillräcklighet. Kommissionen ska översända denna information till nämnden för diskussion och eventuella rekommendationer.

7. Kommissionen ska underlätta erfarenhetsutbytet mellan nationella behöriga myndigheter.

8. Nationella behöriga myndigheter får ge vägledning och råd om genomförandet av denna förordning***, i synnerhet till små och medelstora företag, inbegripet nystartade företag, med beaktande av nämndens och kommissionens vägledning och rådgivning beroende på vad som är lämpligt***. När de nationella behöriga myndigheterna tänker ge vägledning och rådgivning om ett AI-system på områden som omfattas av annan unionslagstiftning, ska vägledningen utarbetas i samråd med de behöriga nationella myndigheterna enligt den unionslagstiftningen i lämpliga fall. ▌

9. Om unionens institutioner, organ och byråer omfattas av denna förordning ska Europeiska datatillsynsmannen fungera som behörig tillsynsmyndighet för dessa.

KAPITEL VIII
EU-DATABAS FÖR ▌ AI-SYSTEM MED HÖG RISK

Artikel 71

EU-databas för AI-system med hög risk som förtecknas i bilaga III

1. Kommissionen ska i samarbete med medlemsstaterna inrätta och upprätthålla en EU-databas som innehåller den information som avses i ***punkterna 2 och 3 i denna artikel*** om AI-system med hög risk som avses i artikel 6.2 och som är registrerade i enlighet med ***artiklarna 49 och 60***. ***När kommissionen fastställer de funktionella specifikationerna för en sådan databas ska den samråda med relevanta experter och när den uppdaterar de funktionella specifikationerna för en sådan databas ska den samråda med nämnden***.

2. De uppgifter som förtecknas i ***avsnitt A i*** bilaga VIII ska föras in i EU-databasen av ***leverantören eller, i tillämpliga fall, av ombudet***.

3. De uppgifter som förtecknas i avsnitt C i bilaga VIII ska föras in i EU-databasen av den spridare som är, eller agerar på uppdrag av, en offentlig myndighet eller byrå eller ett offentligt organ, i enlighet med artikel 49.2 och 49.3.

4. ***Med undantag för det avsnitt som avses i artiklarna 49.4 och 60.5*** ska informationen i den EU-databas ***som registrerats i enlighet med artikel 49*** vara åtkomlig ***och allmänt tillgänglig på ett användarvänligt sätt. Det ska vara lätt att navigera i informationen, som ska vara maskinläsbar. Den information som registreras i enlighet med artikel 60 ska vara tillgänglig endast för marknadskontrollmyndigheter och kommissionen, såvida inte den potentiella leverantören eller leverantören har gett sitt samtycke till att denna information också görs tillgänglig*** för allmänheten.

5. EU-databasen ska innehålla personuppgifter endast i den mån det är nödvändigt för insamling och behandling av information i enlighet med denna förordning. Denna information ska omfatta namnen på och kontaktuppgifter för fysiska personer som ansvarar för att registrera systemet och som har rättslig behörighet att företräda leverantören ***eller spridaren, beroende på vad som är tillämpligt***.

6. Kommissionen ska vara personuppgiftsansvarig för EU-databasen. Den ska ***göra*** tillräckligt tekniskt och administrativt stöd ***tillgängligt för leverantörer, potentiella*** leverantörer ***och spridare***. ***EU-databasen ska uppfylla de tillämpliga tillgänglighetskraven.***

KAPITEL IX
ÖVERVAKNING EFTER UTSLÄPPANDE PÅ MARKNADEN, INFORMATIONSDELNING OCH MARKNADSKONTROLL

Avsnitt 1
Övervakning efter utsläppande på marknaden

Artikel 72

Leverantörers övervakning efter utsläppande på marknaden och planen för övervakning efter utsläppande på marknaden när det gäller AI-system med hög risk

1. Leverantörer ska inrätta och dokumentera ett system för övervakning efter utsläppande på marknaden på ett sätt som står i proportion till AI-teknikens art och riskerna med AI-systemet med hög risk.

2. Systemet för övervakning efter utsläppande på marknaden ska aktivt och systematiskt samla in, dokumentera och analysera relevanta data ***som kan ha*** tillhandahållits av ***spridare eller som kan ha*** samlats in via andra källor om prestandan för AI-systemen med hög risk under hela deras livstid, och som gör det möjligt för leverantören att utvärdera AI-systemens fortlöpande överensstämmelse med kraven i kapitel III avdelning 2. ***I förekommande fall ska övervakningen efter utsläppande på marknaden omfatta en analys av interaktionen med andra AI-system. Denna skyldighet ska inte omfatta känsliga operativa uppgifter om spridare som är brottsbekämpande myndigheter.***

3. Systemet för övervakning efter utsläppande på marknaden ska baseras på en plan för övervakning efter utsläppande på marknaden. Planen för övervakning efter utsläppande på marknaden ska vara en del av den tekniska dokumentation som avses i bilaga IV. Kommissionen ska anta en genomförandeakt med detaljerade bestämmelser som fastställer en mall för planen för övervakning efter utsläppande på marknaden och en förteckning över de element som ska ingå i planen ***senast ... [sex månader före denna förordnings ikraftträdande]***. ***Genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.***

4. För AI-system med hög risk som omfattas av unionens harmoniseringslagstiftning som förtecknas i ***avsnitt A i*** bilaga I ***ska leverantörerna,*** om ett system och en plan för övervakning efter utsläppande på marknaden redan har inrättats enligt den lagstiftningen, ***för att säkerställa enhetlighet, undvika dubbelarbete och minimera ytterligare bördor, ha möjlighet att, beroende på vad som är lämpligt, integrera de nödvändiga*** delar som beskrivs i punkterna 1, 2 och 3 ***med hjälp av den mall som avses i punkt 3 i*** system och planer som redan finns ***enligt den lagstiftningen, förutsatt att en likvärdig skyddsnivå uppnås***.

   Första stycket i denna punkt ska också tillämpas på ▌ AI-system med hög risk som avses i punkt ***5*** i bilaga III och som släpps ut på marknaden eller tas i bruk av ***finansiella*** institut ***som omfattas av krav avseende sina interna styrelseformer, arrangemang eller processer enligt unionslagstiftningen om finansiella tjänster***.

Avsnitt 2

Informationsdelning om allvarliga incidenter

Artikel 73

Rapportering av allvarliga incidenter

1. Leverantörer av AI-system med hög risk som släpps ut på unionsmarknaden ska rapportera alla allvarliga incidenter ***till marknadskontrollmyndigheterna i de medlemsstater där incidenten inträffade***.

.

2. ***Den rapport som avses i punkt 1*** ska göras omedelbart efter det att leverantören har fastställt ett orsakssamband mellan AI-systemet och den ***allvarliga*** incidenten eller ▌ den rimliga sannolikheten för att det finns ett sådant samband och, under alla omständigheter, senast 15 dagar efter det att ***leverantören eller, i tillämpliga fall, spridaren*** fått kännedom om den allvarliga incidenten.

Den rapporteringsperiod som avses i första stycket ska ta hänsyn till hur allvarligt den allvarliga incidenten ***är*** ▌ .

3. ***Trots vad som sägs i punkt 2 i denna artikel ska, i händelse av en utbredd överträdelse eller en allvarlig incident enligt definitionen i artikel 3.44 b, den rapport som avses i punkt 1 i denna artikel tillhandahållas omedelbart och senast två dagar efter det att leverantören eller, i tillämpliga fall, spridaren får kännedom om incidenten.***

5. Trots vad som sägs i punkt 2 ska rapporten, om en person avlider, tillhandahållas omedelbart efter det att leverantören eller spridaren har fastställt, eller så snart den misstänker, ett orsakssamband mellan AI-systemet med hög risk och den allvarliga incidenten, dock senast tio dagar efter den dag då leverantören eller, i tillämpliga fall, spridaren får kännedom om den allvarliga incidenten.

6. Om det är nödvändigt för att säkerställa snabb rapportering får leverantören eller, i tillämpliga fall, spridaren, lämna in en inledande rapport som är ofullständig, följd av en fullständig rapport.

7. Efter rapporteringen av en allvarlig incident i enlighet med punkt 1 ska leverantören utan dröjsmål utföra de nödvändiga utredningarna med avseende på den allvarliga incidenten och det berörda AI-systemet. Detta ska inbegripa en riskbedömning av incidenten och korrigerande åtgärder.

Leverantören ska samarbeta med de behöriga myndigheterna, och i förekommande fall med det berörda anmälda organet, under de utredningar som avses i första stycket, och ska inte utföra någon utredning som inbegriper att ändra det berörda AI-systemet på ett sätt som kan påverka eventuella efterföljande utvärderingar av orsakerna till incidenten, innan den underrättar de behöriga myndigheterna om en sådan åtgärd.

8. Efter att ha mottagit en underrättelse om en ***allvarlig incident enligt artikel 3.44 c ska den berörda*** marknadskontrollmyndigheten informera de nationella offentliga myndigheter eller organ som avses i artikel 77.1. Kommissionen ska utarbeta särskilda vägledning för att underlätta fullgörandet av de skyldigheter som anges i punkt 1 i denna artikel. Dessa riktlinjer ska utfärdas senast … [12 månader efter det att denna förordning har trätt i kraft] ***och ska bedömas regelbundet.***

9. Marknadskontrollmyndigheten ska vidta lämpliga åtgärder i enlighet med vad som föreskrivs i artikel 19 i förordning (EU) 2019/1020 inom sju dagar från den dag som den mottog den underrättelse som avses i punkt 1 i denna artikel och ska följa de underrättelseförfaranden som föreskrivs i den förordningen.

10. För AI-system med hög risk som avses i ▌ bilaga III ***och som*** släpps ut på marknaden eller tas i bruk av leverantörer som ***omfattas av unionslagstifting om rapporteringskyldigheter som är likvärdiga med dem som anges i denna*** förordning ▌ ska anmälan av allvarliga incidenter vara begränsade till dem ***som avses i artikel 3.44 c.***

11. För AI-system med hög risk som utgör säkerhetskomponenter i enheter, eller som själva är enheter, vilka omfattas av förordningarna (EU) 2017/745 och (EU) 2017/746, ska anmälan av allvarliga incidenter begränsas till sådana som avses i artikel 3.44 c i denna förordning och göras till den nationella behöriga myndighet som utsetts för detta ändamål av de medlemsstater där incidenten inträffade.

12. Nationella behöriga myndigheter ska omedelbart underrätta kommissionen om alla allvarliga incidenter, oavsett om de har vidtagit åtgärder med anledning av dessa, i enlighet med artikel 20 i förordning (EU) 2019/1020.

Avsnitt 3

Tillsyn

Artikel 74

Marknadskontroll och kontroll av AI-system på unionsmarkanden

1. Förordning (EU) 2019/1020 ska tillämpas på AI-system som omfattas av denna förordning. För att effektivt kunna kontrollera efterlevnaden av denna förordning gäller följande:

   a) Alla hänvisningar till en ekonomisk aktör inom ramen för förordning (EU) 2019/1020 ska förstås som hänvisningar som omfattar alla operatörer som identifieras ***artikel 2.1*** i den här förordningen.

   b) Alla hänvisningar till en produkt inom ramen för förordning (EU) 2019/1020 ska förstås som hänvisningar som omfattar alla AI-system som omfattas av denna förordning.

2. ***Som en del av sina rapporteringsskyldigheter enligt artikel 34.4 i förordning (EU) 2019/1020*** ska ***marknadskontrollmyndigheterna årligen*** rapportera till kommissionen och berörda nationella konkurrensmyndigheter all information som framkommit i samband med marknadskontrollen och som kan vara av potentiellt intresse för tillämpningen av unionens konkurrenslagstiftning. ***De ska också årligen rapportera till kommissionen om användning av förbjudna metoder som ägt rum det året och om de åtgärder som vidtagits.***

3. För AI-system med hög risk som är relaterade till produkter som omfattas av den unionslagstiftning om harmonisering som förtecknas i avsnitt A i bilaga I ska marknadskontrollmyndigheten vid tillämpning av denna förordning vara den myndighet ansvarig för marknadskontroll som utsetts enligt de rättsakterna. ***Genom undantag från punkt 2 och under lämpliga omständigheter får medlemsstaterna utse en annan berörd myndigheter att fungera som marknadskontrollmyndighet under förutsättning att de säkerställer samordning med de berörda sektorsspecifika marknadskontrollmyndigheter som är ansvariga för tillsynen av de rättsakter som förtecknas i bilaga I.***

4. De förfaranden som avses i artiklarna 79–83 i denna förordning ska inte tillämpas på AI-system som är relaterade till produkter som omfattas av unionslagstiftning om harmonisering som förtecknas i avsnitt A i bilaga I om sådana rättsakter redan föreskriver förfaranden som säkerställer en likvärdig skyddsnivå och har samma syfte. I sådana fall ska dessa relevanta sektorsspecifika förfaranden tillämpas i stället.

5. ***Utan att det påverkar marknadskontrollmyndigheternas befogenheter enligt artikel 14 i förordning (EU) 2019/1020 får marknadskontrollmyndigheterna i syfte att säkerställa en effektiv tillsyn av den här förordningen på distans och i lämpliga fall utöva de befogenheter som avses i artikel 14.4 d och j i den förordningen.***

6. För AI-system ***med hög risk*** som släpps ut på marknaden, tas i bruk eller används av finansinstitut som regleras av unionsrätten om finansiella tjänster ska marknadskontrollmyndigheten vid tillämpning av denna förordning vara den berörda ***nationella*** myndighet som enligt den lagstiftningen ansvarar för den finansiella tillsynen över dessa institut***, i den mån utsläppandet på marknaden, ibruktagandet eller användningen av AI-systemet står i direkt samband med tillhandahållandet av dessa finansiella tjänster.***

7. ***Genom undantag från punkt 6 får en annan berörd myndighet, under lämpliga omständigheter och under förutsättning att samordning säkerställs, av medlemsstaten identifieras som marknadskontrollmyndighet vid tillämpning av denna förordning.***

Nationella marknadskontrollmyndigheter som utövar tillsyn av reglerade kreditinstitut reglerade enligt direktiv 2013/36/EU och som deltar i den gemensamma tillsynsmekanism som inrättats genom förordning (EU) nr 1024/2013, ska utan dröjsmål till Europeiska centralbanken rapportera all information som identifierats i samband med deras marknadskontroll och som kan vara av potentiellt intresse för Europeiska centralbankens tillsynsuppgifter enligt den förordningen.

8. För AI-system ***med hög risk*** som förtecknas i punkt 1 i bilaga III ska medlemsstaterna, i den mån systemen används för brottsbekämpande ändamål, gränsförvaltning och rättvisa och demokrati, ***och för AI-system med hög risk som förtecknas i*** punkterna 6, ***7 och 8*** i bilaga III till denna förordning, till marknadskontrollmyndigheter för tillämpning av denna förordning utse antingen de behöriga tillsynsmyndigheterna för dataskydd enligt ***direktiv (EU) 2016/679 eller*** direktiv (EU) 2016/680***, eller någon annan myndighet som utsetts i enlighet med de villkor som fastställs i*** artiklarna 41–44 ***i*** direktiv ***(EU) 2016/680. Marknadskontrollen ska inte på något sätt påverka de rättsliga myndigheternas oberoende eller på annat sätt inkräkta på deras verksamhet när de agerar inom ramen för sin dömande verksamhet.***

9. När unionens institutioner, byråer eller organ omfattas av denna förordning ska Europeiska datatillsynsmannen fungera som marknadskontrollmyndighet för dessa***, med undantag av när Europeiska unionens domstol agerar i dess rättskipande funktion.***

10. Medlemsstaterna ska underlätta samordningen mellan marknadskontrollmyndigheter som utses enligt denna förordning och andra relevanta nationella myndigheter eller organ som utövar tillsyn över tillämpningen av unionens harmoniseringslagstiftning enligt bilaga I eller annan unionsrätt som kan vara relevant för de AI-system med hög risk som avses i bilaga III.

11. Marknadskontrollmyndigheter och kommissionen ska kunna föreslå gemensamma aktiviteter, inbegripet gemensamma undersökningar, som ska genomföras antingen av marknadskontrollmyndigheterna själva eller av marknadskontrollmyndigheter tillsammans med kommissionen, och som syftar till att främja överensstämmelse, identifiera bristande överensstämmelse, öka medvetenheten och ge vägledning om denna förordning med avseende på specifika kategorier av AI-system med hög risk som befinns utgöra en allvarlig risk i två eller flera medlemsstater i enlighet med artikel 9 i förordning (EU) 2019/1020. AI-byrån ska tillhandahålla samordningsstöd för gemensamma utredningar.

12. Utan att det påverkar de befogenheter som föreskrivs enligt förordning (EU) 2019/1020, och när så är relevant och begränsat till vad som är nödvändigt för att marknadskontrollmyndigheterna ska kunna fullgöra sina uppgifter, ska leverantörer bevilja dessa fullständig åtkomst till den dokumentation och de tränings-, valideringS- och testdataset som används för utvecklingen av AI-system med hög risk, inbegripet, när så är lämpligt och med förbehåll för säkerhetsgarantier, genom applikationsprogrammeringsgränssnitt (API) eller andra relevanta tekniska medel och verktyg som möjliggör fjärråtkomst.

13. Marknadskontrollmyndigheterna ska beviljas tillgång till källkoden för AI-systemet med hög risk på motiverad begäran och endast om båda följande kumulativa villkor är uppfyllda:

a) Tillgång till källkod är nödvändig för att bedöma om ett AI-system med hög risk uppfyller kraven i kapitel III avsnitt 2.

b) Testnings- eller revisionsförfaranden och kontroller som grundas på uppgifter och dokumentation från leverantören har uttömts eller visat sig vara otillräckliga.

14. All information eller dokumentation som har erhållits av marknadskontrollmyndigheter ska behandlas i enlighet med de konfidentialitetskrav som anges i artikel 78.

Artikel 75

Ömsesidigt bistånd, marknadskontroll och kontroll av AI-system för allmänna ändamål

1. Om ett AI-system bygger på en AI-modell för allmänna ändamål och modellen och systemet har utvecklats av samma leverantör ska AI-byrån ha befogenhet att övervaka och kontrollera det AI-systemets efterlevnad av skyldigheter enligt denna förordning. För att utföra sina övervaknings- och tillsynsuppgifter ska AI-byrån ha alla befogenheter som en marknadskontrollmyndighet i den mening som avses i förordning (EU) 2019/1020 har.

2. Om de relevanta marknadskontrollmyndigheterna har tillräckliga skäl att anse att AI-system för allmänna ändamål som kan användas direkt av spridare för minst ett ändamål som klassificeras som utgörande en hög risk enligt denna förordning inte uppfyller de krav som fastställs i denna förordning, ska de samarbeta med AI-byrån för att utföra bedömningar av överensstämmelse och informera nämnden och andra marknadskontrollmyndigheter om detta.

3. Om en marknadskontrollmyndighet inte kan slutföra sina utredningar av AI-system med hög risk på grund av att den inte fått tillgång till viss information avseende AI-modellen, trots att den har vidtagit alla lämpliga åtgärder för att inhämta den informationen, får den lämna en motiverad begäran till AI-byrån, genom vilken tillgång till denna information ska verkställas. I detta fall ska AI-byrån utan dröjsmål, och under alla omständigheter inom 30 dagar, förse den begärande myndigheten med all information som AI-byrån anser vara relevant för att fastställa om ett AI-system med hög risk inte uppfyller kraven. Nationella kontrollmyndigheter ska säkerställa att den information som de erhåller i enlighet med artikel 78 i denna förordning behandlas konfidentiellt. Det förfarande som föreskrivs i kapitel VI i förordning (EU) 2019/1020 ska gälla i tillämpliga delar.

Artikel 76

Marknadskontrollmyndigheters tillsyn av testning under verkliga förhållanden

1. Marknadskontrollmyndigheterna ska ha behörigheter och befogenheter att säkerställa att testning under verkliga förhållanden sker i enlighet med denna förordning.

2. Om testning under verkliga förhållanden utförs för AI-system som står under tillsyn inom ramen för en regulatorisk sandlåda för AI enligt artikel 59, ska marknadskontrollmyndigheterna kontrollera efterlevnaden av bestämmelserna i artikel 60 som en del av sin tillsynsroll för den regulatoriska sandlådan för AI. Dessa myndigheter får, beroende på vad som är lämpligt, tillåta att testning under verkliga förhållanden utförs av leverantören eller den potentiella leverantören med avvikelse från de villkor som anges i artikel 60.4 f och g.

3. Om en marknadskontrollmyndighet har informerats av den potentiella leverantören, leverantören eller någon tredje part om en allvarlig incident eller har andra skäl att anse att villkoren i artiklarna 60 och 61 inte är uppfyllda, får den, beroende på vad som är lämpligt, fatta något av följande beslut på sitt territorium:

a) Tillfälligt avbryta eller avsluta testningen under verkliga förhållanden.

b) Kräva att leverantören eller den potentiella leverantören och användarna ändrar någon aspekt av testningen under verkliga förhållanden.

4. Om en marknadskontrollmyndighet har fattat ett beslut som avses i punkt 3 i denna artikel eller har gjort en invändning i den mening som avses i artikel 60.4 b, ska skälen till beslutet eller invändningen anges i beslutet eller invändningen liksom information om hur leverantören eller den potentiella leverantören kan bestrida beslutet eller invändningen.

5. I tillämpliga fall ska en marknadskontrollmyndighet, om den har fattat ett beslut som avses i punkt 3, meddela skälen till detta till marknadskontrollmyndigheterna i andra medlemsstater där AI-systemet har testats i enlighet med planen för testning.

Artikel 77

Myndigheters befogenheter att skydda grundläggande rättigheter

1. Nationella offentliga myndigheter eller organ som utövar tillsyn över eller kontrollerar efterlevnaden av skyldigheter enligt unionslagstiftning som skyddar grundläggande rättigheter, ***inbegripet rätten till icke-diskriminering,*** i samband med användningen av AI-system med hög risk som avses i bilaga III, ska ha befogenhet att begära och få åtkomst till all dokumentation som skapas eller upprätthålls enligt denna förordning ***på ett språk och i ett format som är lättillgängligt*** när åtkomst till sådan dokumentation är nödvändig för att ***effektivt fullgöra sina*** mandat inom ramen för deras jurisdiktion. Den berörda offentliga myndigheten eller det berörda offentliga organet ska informera marknadskontrollmyndigheten i den berörda medlemsstaten om en sådan begäran.

2. Senast … [***tre*** månader efter det att denna förordning har trätt i kraft] ska varje medlemsstat identifiera de offentliga myndigheter eller organ som avses i punkt 1 och offentliggöra en förteckning över dem ▌. Medlemsstaterna ska anmäla förteckningen till kommissionen och de andra medlemsstaterna och hålla förteckningen uppdaterad.

3. Om den dokumentation som avses i punkt 1 är otillräcklig för att fastställa huruvida ett åsidosättande av skyldigheter enligt unionsrätt som skyddar de grundläggande rättigheterna har ägt rum, får den offentliga myndighet eller det offentliga organ som avses ***i*** punkt 1 lämna en motiverad begäran till marknadskontrollmyndigheten om att testning av AI-systemet med hög risk genom tekniska medel ska organiseras. Marknadskontrollmyndigheten ska organisera testningen i nära samarbete med den begärande offentliga myndigheten eller det begärande offentliga organet inom rimlig tid efter begäran.

4. All information eller dokumentation som de nationella offentliga myndigheter eller organ som avses i punkt 1 i denna artikel erhåller i enlighet med denna artikel ska behandlas i enlighet med de konfidentialitetskrav som fastställs i artikel 78.

Artikel 78

Konfidentiell behandling

1. ***Kommissionen, marknadskontroll***myndigheterna och anmälda organ ***och alla andra fysiska eller juridiska personer*** som deltar i tillämpningen av denna förordning ska***, i enlighet med unionsrätt och nationell rätt,*** respektera konfidentialiteten för den information och de data som de erhåller när de utför sina uppgifter och sin verksamhet på ett sådant sätt att de särskilt skyddar följande***:***

   a) Immateriella rättigheter och en fysisk eller juridisk persons konfidentiella affärsinformation eller företagshemligheter, inklusive källkod, utom i de fall som avses i artikel 5 i Europaparlamentets och rådets direktiv (EU) 2016/943[60] om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs***.***

[60] Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs (EUT L 157, 15.6.2016, s. 1).

b) Ett effektivt genomförande av denna förordning, särskilt med avseende på inspektioner, utredningar eller revisioner. ▌

c) Offentliga och nationella säkerhetsintressen.

d) Genomförandet av straffrättsliga eller administrativa förfaranden.

e) Uppgifter som säkerhetsskyddsklassificerats i enlighet med unionsrätten eller nationell rätt.

2. De myndigheter som deltar i tillämpningen av denna förordning i enlighet med punkt 1 ska endast begära sådana data som är strikt nödvändiga för bedömningen av den risk som AI-system utgör och för utövandet av deras befogenheter i överensstämmelse med denna förordning och förordning (EU) 2019/1020. De ska vidta tillräckliga och effektiva cybersäkerhetsåtgärder för att skydda säkerheten och konfidentialiten för den information och de data som inhämtats, och ska radera inhämtade data så snart dessa inte längre behövs för det ändamål för vilket de inhämtats, i enlighet med tillämplig unionsrätt eller nationell rätt.

3. Utan att det påverkar tillämpningen av punkterna 1 ***och 2*** ska information som på konfidentiell basis utbyts mellan de nationella behöriga myndigheterna eller mellan nationella behöriga myndigheter och kommissionen inte lämnas ut utan föregående samråd med den nationella behöriga myndighet som lämnar informationen och med ***spridaren*** när sådana AI-system med hög risk som avses i punkterna 1, 6 eller 7 i bilaga III används av brottsbekämpande myndigheter, ***gränskontrollmyndigheter***, invandringsmyndigheter eller asylmyndigheter, om ett sådant röjande skulle äventyra allmänna och nationella säkerhetsintressen. ***Detta informationsutbyte ska inte omfatta känsliga operativa uppgifter som rör brottsbekämpande myndigheters, gränskontrollmyndigheters, invandringsmyndigheters eller asylmyndigheters verksamhet.***

Om brottsbekämpande myndigheter, invandringsmyndigheter eller asylmyndigheter är leverantörer av sådana AI-system med hög risk som avses i punkterna 1, 6 och 7 i bilaga III ska den tekniska dokumentation som avses i bilaga IV finnas kvar i dessa myndigheters lokaler. Dessa myndigheter ska säkerställa att de marknadskontrollmyndigheter som avses i artikel 74.8 och 74.9, beroende på vad som är tillämpligt, på begäran omedelbart kan få åtkomst till eller få en kopia av dokumentationen. Endast personal vid marknadskontrollmyndigheten som innehar säkerhetsgodkännande på tillräckligt hög nivå ska ha åtkomst till denna dokumentation eller kopior av denna.

4. Punkterna 1***, 2*** och 3 påverkar inte kommissionens, medlemsstaternas och ***deras relevanta myndigheters samt*** anmälda organs rättigheter och skyldigheter när det gäller att utbyta information och utfärda varningar***, inbegripet i samband med gränsöverskridande samarbete,*** och inte heller påverkas de berörda personernas straffrättsliga skyldighet att lämna information enligt medlemsstaternas straffrätt.

5. Kommissionen och medlemsstaterna får, om det är nödvändigt ***och om det är förenligt med relevanta bestämmelser i internationella avtal och handelsavtal***, utbyta konfidentiell information med de tillsynsmyndigheter i tredjeländer med vilka de har slutit bilaterala eller multilaterala avtal om konfidentialitet som garanterar en tillräcklig nivå av konfidentialitet.

Artikel 79

Förfaranden för att hantera AI-system som utgör en risk på nationell nivå

1. AI-system som utgör en risk ska förstås som en produkt som utgör en risk enligt definitionen i artikel 3.19 i förordning (EU) 2019/1020 i den mån de utgör risker för personers ▌ hälsa eller säkerhet eller grundläggande rättigheter.

2. Om en medlemsstats marknadskontrollmyndighet har tillräckliga skäl att anse att ett AI-system utgör en sådan risk som avses i punkt 1 i denna artikel, ska ***den*** utvärdera om det berörda AI-systemet är förenligt med alla krav och skyldigheter som fastställs i denna förordning. ***Särskild uppmärksamhet ska ägnas åt AI-system som utgör en risk för grupper av sårbara personer som avses i artikel 5. Om risker*** för personers grundläggande rättigheter ***identifieras*** ska marknadskontrollsmyndigheten även omedelbart informera ***och till fullo samarbeta med*** de berörda nationella offentliga myndigheter eller organ som avses i artikel 77.1. De berörda operatörerna ska vid behov samarbeta med marknadskontroll***myndigheten*** och andra nationella offentliga myndigheter eller organ som avses i artikel 77.1.

Om marknadskontrollsmyndigheten eller***, när så är lämpligt,*** marknadskontrollsmyndigheten ***i samarbete med den nationella offentliga myndighet som avses i artikel 77.1,*** vid utvärderingen konstaterar att AI-systemet inte uppfyller kraven och skyldigheterna i denna förordning ska den utan ***onödigt*** dröjsmål kräva att berörda operatörer vidtar alla lämpliga korrigerande åtgärder för att AI-systemet ska uppfylla dessa krav, dra tillbaka AI-systemet från marknaden eller återkalla det inom en ***period*** som marknadskontrollsmyndigheten ***får fastställa, och i alla händelser senast inom 15 arbetsdagar eller såsom fastställts i unionens relevanta harmoniseringslagstiftning.***

Marknadskontrollmyndigheten ska informera det berörda anmälda organet om detta. Artikel 18 i förordning (EU) 2019/1020 ska tillämpas på de åtgärder som avses i andra stycket i denna punkt.

3. Om marknadskontrollmyndigheten anser att den bristande överensstämmelsen inte bara gäller det nationella territoriet, ska den ***utan onödigt dröjsmål*** informera kommissionen och de andra medlemsstaterna om utvärderingsresultaten och om de åtgärder som den har ålagt operatören att vidta.

4. Operatören ska säkerställa att alla lämpliga korrigerande åtgärder vidtas i fråga om alla berörda AI-system som den har tillhandahållit på unionsmarknaden.

5. Om operatören av ett AI-system inte vidtar lämpliga korrigerande åtgärder inom den tid som avses i punkt 2, ska marknadskontrollmyndigheten vidta alla lämpliga provisoriska åtgärder för att förbjuda eller begränsa tillhandahållandet ***eller ibruktagandet*** av AI-systemet på sin nationella marknad, dra tillbaka produkten ***eller det fristående AI-systemet*** från den marknaden eller återkalla det. Myndigheten ska ***utan onödigt dröjsmål anmäla*** dessa åtgärder ▌ till kommissionen och de andra medlemsstaterna.

6. I den ***anmälan*** som avses i punkt 5 ska alla tillgängliga data ingå, särskilt den ***information*** som krävs för att kunna identifiera det AI-system som inte uppfyller kraven, dess ursprung ***och leveranskedjan***, vilken typ av bristande överensstämmelse som görs gällande och den risk systemet utgör, vilken typ av nationell åtgärd som vidtagits och dess varaktighet samt den berörda operatörens synpunkter. Marknadskontrollmyndigheterna ska särskilt ange om den bristande överensstämmelsen beror en eller flera av följande orsaker:

   a) Bristande efterlevnad av det förbud mot AI-metoder som avses i artikel 5.

   b) AI-systemet ***med hög risk*** uppfyller inte kraven i kapitel III avsnitt 2.

   c) Brister i de harmoniserade standarderna eller gemensamma specifikationerna som avses i artiklarna 40 och 41 som ger presumtion om överensstämmelse.

   d) Bristande efterlevnad av artikel 50.

7. Andra marknadskontrollmyndigheter i medlemsstaterna än marknadskontrollmyndigheten i den medlemsstat som inledde förfarandet ska utan ***onödigt*** dröjsmål informera kommissionen och de andra medlemsstaterna om alla vidtagna åtgärder och eventuella kompletterande uppgifter som de har tillgång till med avseende på AI-systemets bristande överensstämmelse och, vid oenighet om den anmälda nationella åtgärden, om sina invändningar.

8. Åtgärden ska anses vara berättigad om ingen ***marknadskontrollmyndighet i*** en medlemsstat eller kommissionen har gjort invändningar inom tre månader efter mottagandet av den ***anmälan*** som avses i punkt 5 mot en provisorisk åtgärd som vidtagits av en ***marknadskontrollmyndighet i en annan*** medlemsstat. Detta ska inte påverka den berörda operatörens processuella rättigheter i enlighet med artikel 18 i förordning (EU) 2019/1020. ***Den tremånadersperiod som avses i detta stycke ska minskas till 30 dagar vid bristande efterlevnad av förbudet mot de AI-metoder som avses i artikel 5 i denna förordning.***

9. Marknadskontrollmyndigheterna i medlemsstaterna ska säkerställa att lämpliga begränsande åtgärder, till exempel att produkten ***eller AI-systemet*** dras tillbaka från marknaden, vidtas i fråga om den berörda produkten ***eller det berörda AI-systemet*** utan ***onödigt*** dröjsmål.

Artikel 80

Förfarande för hantering av AI-system som av leverantören klassificeras som AI-system utan hög risk vid tillämpning av bilaga III

1. *Om en marknadskontrollmyndighet har tillräckliga skäl att anse att ett AI-system som av leverantören klassificeras som av AI-system utan hög risk i enlighet med artikel 6.3 I faktiskt är ett högrisksystem, ska marknadskontrollmyndigheten genomföra en utvärdering av det berörda AI-systemet med avseende på dess klassificering som AI-system med hög risk på grundval av de villkor som anges i artikel 6.3 och kommissionens riktlinjer.*

2. *Om marknadskontrollmyndigheten vid utvärderingen konstaterar att det berörda AI-systemet är ett system med hög risk ska den utan onödigt dröjsmål ålägga den berörda leverantören att vidta alla nödvändiga åtgärder för att AI-systemet ska uppfylla de krav och skyldigheter som fastställs i denna förordning samt vidta lämpliga korrigerande åtgärder inom en period som marknadskontrollmyndigheten får föreskriva.*

3. *Om marknadskontrollmyndigheten anser att användningen av det berörda AI-systemet inte är begränsad till det nationella territoriet, ska den utan onödigt dröjsmål informera kommissionen och de andra medlemsstaterna om utvärderingsresultaten och om de åtgärder som den har ålagt operatören att vidta.*

4. Leverantören ska säkerställa att alla nödvändiga åtgärder vidtas för att AI-systemet ska uppfylla de krav och skyldigheter som fastställs i denna förordning. Om leverantören av ett berört AI-system inte bringar AI-systemet i överensstämmelse med dessa krav och skyldigheter inom den period som avses i punkt 2 i denna artikel ska leverantören bli föremål för sanktionsavgifter i enlighet med artikel 99.

5. Leverantören ska säkerställa att alla lämpliga korrigerande åtgärder vidtas i fråga om alla berörda AI-system som den har tillhandahållit på unionsmarknaden.

6. Om leverantören av det berörda AI-systemet inte vidtar lämpliga korrigerande åtgärder inom den period som avses i punkt 2 i denna artikel ska artikel 79.5–75.9 tillämpas.

7. Om marknadskontrollmyndigheten vid utvärderingen enligt punkt 1 i denna artikel fastställer att AI-systemet av leverantören felaktigt klassificerats som ett system utan hög risk i syfte att kringgå tillämpningen av kraven i kapitel III avsnitt 2, ska leverantören bli föremål för sanktionsavgifter i enlighet med artikel 99.

8. ***När marknadskontrollmyndigheterna utövar sina befogenheter att övervaka tillämpningen av denna artikel, och i enlighet med artikel 11 i förordning (EU) 2019/1020, får de utföra lämpliga kontroller, med särskilt beaktande av information som lagras i den EU-databas som avses i artikel 71 i den här förordningen.***

Artikel 81

Unionsförfarande för skyddsåtgärder

1. Om ***marknadskontrollmyndigheten*** i en medlemsstat inom tre månader efter mottagandet av den anmälan som avses i artikel 79.5***, eller inom 30 dagar vid bristande efterlevnad av förbudet mot de AI-metoder som avses i artikel 5,*** har gjort invändningar mot en åtgärd som vidtagits av ***marknadskontrollmyndigheten*** i en annan medlemsstat, eller om kommissionen anser att åtgärden strider mot unionsrätten, ska kommissionen utan ***onödigt*** dröjsmål inleda samråd med den berörda medlemsstatens ***marknadskontrollmyndighet*** och operatören eller operatörerna och ska utvärdera den nationella åtgärden. På grundval av utvärderingsresultaten ska kommissionen besluta om den nationella åtgärden är berättigad eller inte inom ***sex*** månader***, eller inom 60 dagar vid bristande efterlevnad av förbudet mot de AI-metoder som avses i artikel 5, från*** den anmälan som avses i artikel 79.5 och meddela beslutet till ***marknadskontrollmyndigheten*** i den berörda medlemsstaten. ***Kommissionen ska också underrätta alla de övriga marknadskontrollmyndigheterna om ett sådant beslut.***

2. Om kommissionen anser att den ***åtgärd som vidtagits av den berörda medlemsstaten*** är motiverad ska samtliga medlemsstater ***säkerställa att de vidtar lämpliga restriktiva*** åtgärder ***med avseende på det berörda*** AI-systemet***, såsom att kräva att AI-systemet dras tillbaka*** från deras marknad ***utan onödigt dröjsmål,*** och underrätta kommissionen om detta. Om kommissionen anser att den nationella åtgärden är omotiverad ska den berörda medlemsstaten dra tillbaka åtgärden ***och underrätta kommissionen om detta.***

3. Om den nationella åtgärden anses vara berättigad och AI-systemets bristande överensstämmelse kan tillskrivas brister i de harmoniserade standarder eller gemensamma specifikationer som avses i artiklarna 40 och 41 i denna förordning, ska kommissionen tillämpa det förfarande som föreskrivs i artikel 11 i förordning (EU) nr 1025/2012.

Artikel 82

AI-system som uppfyller kraven och som utgör en risk

1. Om en marknadskontrollmyndighet i en medlemsstat har gjort en utvärdering enligt artikel 79 och***, efter samråd med den nationella offentliga myndighet som avses i artikel 77.1,*** konstaterar att ett AI-systemet ***med hög risk*** uppfyller kraven i denna förordning men ändå utgör en risk för personers hälsa och säkerhet, ▌ för de grundläggande rättigheterna eller för andra aspekter av skyddet av allmänintresset, ska den ålägga den berörda operatören att, ***utan onödigt dröjsmål*** och inom en ▌ period ▌ som den får fastställa, vidta alla lämpliga åtgärder för att säkerställa att det berörda AI-systemet när det släpps ut på marknaden eller tas i bruk inte längre utgör en sådan risk.

2. Leverantören eller en annan berörd operatör ska säkerställa att korrigerande åtgärder vidtas i fråga om alla berörda AI-system som den har tillhandahållit på marknaden i unionen inom den tidsplan som föreskrivs av marknadskontrollmyndigheten i den medlemsstat som avses i punkt 1.

3. ***Medlemsstaterna*** ska omedelbart informera kommissionen och de andra medlemsstaterna om ett konstaterande enligt punkt 1. Den informationen ska innehålla alla tillgängliga närmare uppgifter, särskilt de data som krävs för att kunna identifiera det berörda AI-systemet, dess ursprung och leveranskedja, den risk som AI-systemet utgör samt vilken typ av nationella åtgärder som vidtagits och deras varaktighet.

4. Kommissionen ska utan ***onödigt*** dröjsmål inleda samråd med den ***berörda*** medlemsstaten eller de berörda medlemsstaterna och de berörda operatörerna samt utvärdera de nationella åtgärderna. På grundval av utvärderingsresultaten ska kommissionen besluta om åtgärden är berättigad, och vid behov föreslå andra lämpliga åtgärder.

5. Kommissionen ska ***omedelbart meddela*** sitt beslut till de ***berörda*** medlemsstaterna ***och till de berörda operatörerna. Den ska också informera övriga medlemsstater.***

Artikel 83

Formell bristande överensstämmelse

1. Om marknadskontrollmyndigheten i en medlemsstat konstaterar något av följande ska den ålägga den berörda leverantören att åtgärda den bristande överensstämmelsen ***inom en tid som den får föreskriva***:

   a) ***CE***-märkningen har anbringats i strid med artikel 48.

   b) ***CE***-märkning saknas.

   c) Det har inte upprättats någon EU-försäkran om överensstämmelse.

   d) EU-försäkran om överensstämmelse har inte upprättats på ett korrekt sätt.

   e) Registreringen i EU-databasen har inte genomförts.

   f) I tillämpliga fall har ett ombud inte utsetts.

   g) Teknisk dokumentation är inte tillgänglig.

2. Om den bristande överensstämmelse som avses i punkt 1 kvarstår ska ***marknadskontrollmyndigheten i den*** berörda medlemsstaten vidta ***lämpliga och proportionerliga*** åtgärder för att begränsa eller förbjuda tillhandahållandet av AI-systemet med hög risk på marknaden eller säkerställa att det ***utan dröjsmål*** återkallas eller dras tillbaka från marknaden.

Artikel 84

Unionsstödstrukturer för provning av AI

1. Kommissionen ska utse en eller flera unionsstödstrukturer för provning av AI i enlighet med artikel 21 i förordning (EU) 2019/1020 på AI-området.

2. Utan att det påverkar de uppgifter som avses i punkt 1 ska unionsstödstrukturerna för provning av AI även tillhandahålla oberoende teknisk eller vetenskaplig rådgivning på begäran av nämnden, kommissionen eller marknadskontrollmyndigheterna.

Avsnitt 4

Rättsmedel

Artikel 85

Rätt att lämna in klagomål till en marknadskontrollmyndighet

Utan att det påverkar andra administrativa eller rättsliga rättsmedel får varje fysisk eller juridisk person som har skäl att anse att bestämmelserna i denna förordning har överträtts lämna motiverade klagomål till den berörda marknadskontrollmyndigheten.

I enlighet med förordning (EU) 2019/1020 ska sådana klagomål beaktas vid genomförandet av marknadskontrollen och hanteras i enlighet med de särskilda förfaranden som fastställts för detta av marknadskontrollmyndigheterna.

Artikel 86

Rätt till förklaring av individuellt beslutsfattande

1. *Varje berörd person som är föremål för ett beslut som fattas av spridaren på grundval av utdata från ett AI-system med hög risk som förtecknas i bilaga III, med undantag för system som förtecknas i punkt 2 i den bilagan, och som har rättslig verkan eller på liknande sätt i betydande grad påverkar den personen på ett sätt som de anser ha en negativ inverkan på deras hälsa, säkerhet eller grundläggande rättigheter, ska ha rätt att erhålla tydliga och meningsfulla förklaringar av AI-systemets roll i beslutsförfarandet och de viktigaste delarna av det beslut som fattats.*

2. *Punkt 1 ska inte tillämpas på användning av AI-system för vilka undantag från eller begränsningar av skyldigheten enligt punkt 1 följer av unionsrätten eller nationell rätt i överensstämmelse med unionsrätten.*

3. *Denna artikel ska endast tillämpas i den utsträckning som den rättighet som avses i punkt 1 inte på annat sätt föreskrivs i unionsrätten.*

Artikel 87

Rapportering av överträdelser och skydd av personer som rapporterar överträdelser

Direktiv (EU) 2019/1937 ska tillämpas på rapportering av överträdelser av denna förordning och skydd för personer som rapporterar om sådana överträdelser.

Avsnitt 5

Tillsyn, utredning, efterlevnadskontroll och övervakning av leverantörer av AI-modeller för allmänna ändamål

Artikel 88

Kontroll av efterlevnaden av skyldigheterna för leverantörer av AI-modeller för allmänna ändamål

1. Kommissionen ska ha exklusiv befogenhet att övervaka och verkställa kapitel V, med beaktande av rättssäkerhetsgarantierna enligt artikel 94. Kommissionen ska anförtro genomförandet av dessa uppgifter till AI-byrån, utan att det påverkar kommissionens organisationsbefogenheter och befogenhetsfördelningen mellan medlemsstaterna och unionen på grundval av fördragen.

2. Utan att det påverkar tillämpningen av artikel 75.3 får marknadskontrollmyndigheterna begära att kommissionen utövar de befogenheter som fastställs i detta avsnitt, om detta är nödvändigt och proportionellt för att hjälpa dem att fullgöra sina uppgifter enligt denna förordning.

Artikel 89

Övervakningsåtgärder

1. För att utföra de uppgifter som tilldelas den enligt detta avsnitt får AI-byrån vidta nödvändiga åtgärder för att övervaka att leverantörer av AI-modeller för allmänna ändamål genomför och efterlever denna förordning på ett effektivt sätt, inbegripet deras efterlevnad av godkända uppförandekoder.

2. Leverantörer i efterföljande led ska ha rätt att lämna in ett klagomål om överträdelse av denna förordning. Ett klagomål ska vara vederbörligen motiverat och innehålla åtminstone följande uppgifter:

a) Kontaktpunkten för leverantören av den berörda AI-modellen för allmänna ändamål.

b) En beskrivning av relevanta fakta, de berörda bestämmelserna i denna förordning och skälet till att leverantören i efterföljande led anser att leverantören av den berörda AI-modellen för allmänna ändamål har överträtt denna förordning.

c) All övrig information som den leverantör i efterföljande led som skickade begäran anser vara relevant, inbegripet, i förekommande fall, information som samlats in på eget initiativ.

Artikel 90

Varningar från den vetenskapliga panelen om systemrisker

1. Den vetenskapliga panelen får lämna en kvalificerad varning till AI-byrån om den har anledning att misstänka att

a) en AI-modell för allmänna ändamål utgör en konkret identifierbar risk på unionsnivå, eller,

b) en AI-modell för allmänna ändamål uppfyller de krav som avses i artikel 51.

2. Efter en sådan kvalificerad varning får kommissionen, genom AI-byrån och efter att ha informerat nämnden, utöva de befogenheter som fastställs i detta kapitel i syfte att bedöma ärendet. AI-byrån ska informera nämnden om alla åtgärder i enlighet med artiklarna 91–94.

3. En kvalificerad varning ska vara vederbörligen motiverad och innehålla åtminstone följande uppgifter:

a) Kontaktpunkten för leverantören av AI-modellen för allmänna ändamål med systemrisk.

b) En beskrivning av relevanta fakta och skälen till den vetenskapliga panelens varning.

c) All övrig information som den vetenskapliga panelen anser vara relevant, inbegripet, i förekommande fall, information som samlats in på eget initiativ.

Artikel 91

Befogenhet att begära dokumentation och information

1. Kommissionen får begära att leverantören av den berörda AI-modellen för allmänna ändamål tillhandahåller den dokumentation som utarbetats av leverantören i enlighet med artiklarna 53 och 55, eller all ytterligare information som är nödvändig för att bedöma leverantörens efterlevnad av denna förordning.

2. Innan begäran om information skickas får AI-byrån inleda en strukturerad dialog med leverantören av AI-modellen för allmänna ändamål.

3. På en vederbörligen motiverad begäran från den vetenskapliga panelen får kommissionen utfärda en begäran om information till en leverantör av en AI-modell för allmänna ändamål, om tillgången till information är nödvändig och proportionell för fullgörandet av den vetenskapliga panelens uppgifter enligt artikel 68.2.

4. Begäran om information ska innehålla uppgifter om den rättsliga grunden för och syftet med begäran, en specifikation av vilken information som begärs, en tidsfrist inom vilken åtkomsten ska tillhandahållas samt de sanktionsavgifter som föreskrivs i artikel 101 för tillhandahållande av oriktig, ofullständig eller vilseledande information.

5. Leverantören av den berörda AI-modellen för allmänna ändamål, eller dennes företrädare, ska tillhandahålla den begärda informationen. När det gäller juridiska personer, företag eller firmor, eller leverantören inte är en juridisk person, ska de personer som är behöriga att företräda dem enligt lag eller stadgar tillhandahålla den begärda informationen på uppdrag av leverantören av den berörda AI-modellen för allmänna ändamål. I behörig ordning befullmäktigade advokater får lämna information på sina huvudmäns vägnar. Huvudmännen förblir dock fullt ut ansvariga om den tillhandahållna informationen är ofullständig, oriktig eller vilseledande.

Artikel 92

Befogenhet att genomföra utvärderingar

1. AI-byrån får, efter samråd med nämnden, genomföra utvärderingar av den berörda AI-modellen för allmänna ändamål i syfte att

a) bedöma leverantörens efterlevnad av skyldigheterna enligt denna förordning, om den information som samlats in i enlighet med artikel 91 är otillräcklig, eller,

b) undersöka systemrisker på unionsnivå för AI-modeller för allmänna ändamål med systemrisk, särskilt efter en kvalificerad rapport från den vetenskapliga panelen i enlighet med artikel 89.1 a.

2. Kommissionen får besluta att utse oberoende experter som ska utföra utvärderingar på dess vägnar, inbegripet från den vetenskapliga panel som inrättats i enlighet med artikel 68. Oberoende experter som utses för denna uppgift ska uppfylla de kriterier som anges i artikel 68.2.

3. Vid tillämpningen av punkt 1 får kommissionen begära åtkomst till den berörda AI-modellen för allmänna ändamål genom applikationsprogrammeringsgränssnitt (API) eller ytterligare lämpliga tekniska medel och verktyg, inbegripet källkod.

4. I begäran om åtkomst ska anges den rättsliga grunden, syftet med och skälen till begäran, den tidsfrist inom vilken åtkomsten ska tillhandahållas samt de sanktionsavgifter som föreskrivs i artikel 101 för underlåtenhet att ge åtkomst.

5. Leverantörerna av den berörda AI-modellen för allmänna ändamål och, när det gäller juridiska personer, företag eller firmor, eller om de inte är juridiska personer, de personer som är behöriga att företräda dem enligt lag eller stadgar, ska tillhandahålla den begärda åtkomsten på uppdrag av leverantören av den berörda AI-modellen för allmänna ändamål.

6. Kommissionen ska anta genomförandeakter som fastställer närmare arrangemang och villkor för utvärderingarna, inbegripet närmare bestämmelser för deltagande av oberoende experter, och förfarandet för att välja ut dem. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

7. Innan AI-byrån begär åtkomst till den berörda AI-modellen för allmänna ändamål får den inleda en strukturerad dialog med leverantören av AI-modellen för allmänna ändamål för att samla in mer information om den interna testningen av modellen, interna skyddsåtgärder för att förebygga systemrisker och andra interna förfaranden och åtgärder som leverantören har vidtagit för att minska sådana risker.

Artikel 93

Befogenhet att begära åtgärder

1. När det är nödvändigt och lämpligt får kommissionen a) begära att leverantörerna vidtar lämpliga åtgärder för att fullgöra de skyldigheter som föreskrivs i artikel 53,

b) kräva att en leverantör ska genomföra riskreducerande åtgärder, om den utvärdering som utförts i enlighet med artikel 92 har gett upphov till allvarliga och väl underbyggda farhågor om en systemrisk på unionsnivå,

c) begränsa tillhandahållandet på marknaden, dra tillbaka eller återkalla modellen.

2. Innan en åtgärd begärs får AI-byrån inleda en strukturerad dialog med leverantören av AI-modellen för allmänna ändamål.

3. Om leverantören av AI-modellen för allmänna ändamål med systemrisk under den strukturerade dialog som avses i punkt 2 erbjuder att åta sig att genomföra riskreducerande åtgärder för att hantera en systemrisk på unionsnivå, får kommissionen genom beslut göra dessa åtaganden bindande och förklara att det inte finns några ytterligare skäl till åtgärder.

Artikel 94

Processuella rättigheter för ekonomiska operatörer av AI-modellen med allmänna ändamål

Artikel 18 i förordning (EU) 2019/1020 ska i tillämpliga delar gälla för leverantörer av AI-modellen för allmänna ändamål, utan att det påverkar de mer specifika processuella rättigheter som föreskrivs i denna förordning.

KAPITEL X
UPPFÖRANDEKODER OCH RIKTLINJER

Artikel 95

Uppförandekod för frivillig tillämpning av specifika krav

1. ***AI-byrån*** och medlemsstaterna ska uppmuntra och underlätta utarbetandet av uppförandekoder, ***inbegripet tillhörande styrningsmekanismer,*** som är avsedda att främja frivillig tillämpning på AI-system, utom AI-system med hög risk, av ***vissa eller alla av*** de krav som anges i kapitel III avsnitt 2, ***med beaktande av tillgängliga tekniska lösningar och bästa branschpraxis som möjliggör tillämpning av sådana krav.***

2. ***AI-byrån*** och ***medlemsstaterna*** ska ▌ underlätta utarbetandet av uppförandekoder ***för*** frivillig tillämpning, ***inbegripet av spridare***, ***av särskilda krav på alla*** AI-system, ***på grundval av tydliga mål och nyckelprestationsindikatorer för att mäta uppnåendet av dessa mål, inbegripet men inte begränsat till, sådana inslag som***

a) tillämpliga inslag som föreskrivs i unionens etiska riktlinjer för tillförlitlig AI,

b) bedöma och minimera AI-systemens inverkan på miljömässig hållbarhet, inbegripet när det gäller energieffektiv programmering och teknik för effektiv utformning, träning och användning av AI,

c) främja AI-kompetens, särskilt hos personer som arbetar med utveckling, drift och användning av AI,

d) underlätta en inkluderande och diversifierad utformning av AI-system, bland annat genom att inrätta inkluderande och diversifierade utvecklingsteam och främja berörda parters deltagande i den processen,

e) bedöma och förebygga AI-systemens negativa inverkan på sårbara personer eller grupper av sårbara personer, inbegripet när det gäller tillgänglighet för personer med funktionsnedsättning, samt på jämställdheten.

3. Uppförandekoder får utarbetas av enskilda leverantörer ***eller spridare*** av AI-system eller av organisationer som företräder dem eller av båda dessa, inbegripet genom att ***spridare*** och eventuella berörda parter och deras representativa organisationer involveras, ***inbegripet organisationer i civilsamhället och den akademiska världen***. Uppförandekoder får omfatta ett eller flera AI-system med beaktande av likheten mellan de berörda systemens avsedda ändamål.

4. När ***AI-byrån*** och ***medlemsstaterna*** uppmuntrar och underlättar utarbetandet av uppförandekoder ska de ta hänsyn till de särskilda intressen och behov som ***små och medelstora företag, inbegripet*** nystartade företag, har.

Artikel 96

Riktlinjer från kommissionen om genomförandet av denna förordning

1. Kommissionen ska utarbeta riktlinjer för det praktiska genomförandet av denna förordning, särskilt avseende

a) tillämpningen av de krav och skyldigheter som avses i artiklarna 8- 15 och i artikel 25,

b) de förbjudna metoder som avses i artikel 5,

c) det praktiska genomförandet av bestämmelserna om väsentliga ändringar,

d) det praktiska genomförandet av de transparensskyldigheter som fastställs i artikel 50,

e) detaljerad information om denna förordnings förhållande till den unionsharmoniseringslagstiftning som förtecknas i bilaga I samt med annan relevant unionsrätt, inbegripet när det gäller enhetlighet i efterlevnaden av den,

f) tillämpningen av definitionen av ett AI-system enligt artikel 3.1.

När kommissionen utfärdar sådana riktlinjer ska den ägna särskild uppmärksamhet åt behoven hos små och medelstora företag, inbegripet nystartade företag, lokala offentliga myndigheter och sektorer som mest sannolikt kommer att beröras av denna förordning.

De riktlinjer som avses i första stycket ska ta vederbörlig hänsyn till den allmänt erkända tidigare kända tekniken när det gäller AI samt till relevanta harmoniserade standarder och gemensamma specifikationer som avses i artiklarna 40 och 41, eller till de harmoniserade standarder eller tekniska specifikationer som fastställs i enlighet med unionens harmoniseringslagstiftning.

2. På begäran av medlemsstaterna eller AI-byrån, eller på eget initiativ, ska kommissionen uppdatera redan antagna riktlinjer när det anses nödvändigt.

KAPITEL XI
DELEGERING AV BEFOGENHETER OCH KOMMITTÉFÖRFARANDE

Artikel 97

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den ***befogenhet att anta delegerade akter*** som avses i artiklarna 6.6, 7.1 och 7.3, 11.3, 43.5 och 43.6, 47.5, ***51.3, 52.4 samt 53.5 och 53.6*** ska ges till kommissionen för en period på ***fem år från och med den*** ... ***[dagen för ikraftträdandet*** av denna förordning]. ***Kommissionen ska utarbeta en rapport om delegeringen av befogenhet senast nio månader före utgången av perioden på fem år. Delegeringen av befogenhet ska genom tyst medgivande förlängas med perioder av samma längd, såvida inte Europaparlamentet eller rådet motsätter sig en sådan förlängning senast tre månader före utgången av perioden i fråga.***

3. Den delegering av befogenhet som avses i artiklarna 6.6, 7.1 och 7.3, 11.3, 43.5 och 43.6, 47.5, ***51.3, 52.4 samt 53.5 och 53.6*** får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i ***Europeiska unionens officiella tidning***, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artiklarna 6.6, 7.1 och 7.3, 11.3, 43.5 och 43.6, 47.5, ***51.3, 52.4, 53.5 och 53.6*** ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av tre månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med tre månader på Europaparlamentets eller rådets initiativ.

Artikel 98

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

KAPITEL XII
SANKTIONER

Artikel 99
Sanktioner

1. Medlemsstaterna ska i enlighet med de villkor som fastställs i denna förordning fastställa bestämmelser om sanktioner ***och andra efterlevnadsåtgärder som också kan innefatta varningar och icke-monetära åtgärder*** som ska tillämpas vid ***operatörers*** överträdelser av bestämmelserna i denna förordning och vidta alla nödvändiga åtgärder för att se till att de tillämpas korrekt och effektivt ***varvid hänsyn ska tas till de riktlinjer som kommissionen utfärdat i enlighet med*** artikel 96. Sanktionerna ska vara effektiva, proportionella och avskräckande. De ska ta hänsyn till ***små och medelstora företags, inbegripet nystartade företags***, ▌ intressen och deras ekonomiska bärkraft.

2. Medlemsstaterna ska ***utan dröjsmål och senast den dag då förordningen börjar tillämpas*** underrätta kommissionen om de regler om påföljder och andra efterlevnadsåtgärder som avses i punkt 1 och utan dröjsmål underrätta den om eventuella senare ändringar av dem.

3. ***Bristande efterlevnad av förbudet mot de AI-metoder som avses i artikel 5*** ska vara föremål för administrativa sanktionsavgifter på upp till ***35 000 000*** EUR eller, om överträdelsen begås av ***ett företag***, upp till 7 % av dess totala globala årsomsättning för det föregående räkenskapsåret, beroende på vilket som är högst.

4. ***Ett*** AI-systems bristande efterlevnad av något ***av följande bestämmelser som hör samman med operatörer eller anmälda organ*** utöver de bestämmelser som fastställs i artikel 5 ska medföra administrativa sanktionsavgifter på upp till ***15 000 000*** EUR eller, om överträdelsen begås av ett företag, upp till ***3 %*** av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst:

   a) Leverantörernas skyldigheter enligt artikel 16.

   b) Ombudens skyldigheter enligt artikel 22.

   c) Importörernas skyldigheter enligt artikel 23.

d) Distributörernas skyldigheter enligt artikel 24.

e) Spridarnas skyldigheter enligt artikel 26.

f) Kraven och skyldigheterna för anmälda organ enligt artiklarna 31, 33.1, 33.3, 33.4 eller 34.

g) Transparensskyldigheterna för leverantörer och användare enligt artikel 50.

5. Tillhandahållande av oriktig, ofullständig eller vilseledande information till anmälda organ eller nationella behöriga myndigheter som svar på en begäran ska medföra administrativa sanktionsavgifter på upp till ***7 500 000*** EUR eller, om överträdelsen begås av ett företag, upp till ***1*** % av dess totala globala årsomsättning för det föregående räkenskapsåret, beroende på vilket som är högst.

6. När det gäller små och medelstora företag, inbegripet nystartade företag, ska varje sanktionsavgift som avses i denna artikel uppgå till högst de procentsatser eller belopp som avses i punkterna 3, 4 och 5, beroende på vilket belopp som är lägre.

7. Vid beslut om ***huruvida administrativa sanktionsavgifter ska åläggas och beslut*** om storleken på den administrativa sanktionsavgiften i varje enskilt fall ska alla relevanta omständigheter i den specifika situationen beaktas och vederbörlig hänsyn, ***i förekommande fall,*** tas till

a) överträdelsens art, svårighetsgrad och varaktighet samt dess konsekvenser ***med beaktande av det berörda AI-systemets syfte samt, när så är lämpligt, antalet berörda personer och omfattningen av den skada som de har lidit,***

b) huruvida administrativa sanktionsavgifter redan har tillämpats av andra marknadskontrollmyndigheter ***i en eller flera medlemsstater*** på samma operatör för samma överträdelse,

c) huruvida administrativa sanktionsavgifter redan har tillämpats av andra myndigheter på samma operatör för överträdelser av annan unionsrätt eller nationell rätt, när sådana överträdelser beror på samma verksamhet eller underlåtenhet som utgör en relevant överträdelse av denna förordning,

d) storleken på, ***årsomsättningen*** och marknadsandelen för den operatör som begått överträdelsen,

e) eventuell annan försvårande eller förmildrande faktor som är tillämplig på omständigheterna i fallet, såsom ekonomisk vinst som görs eller förlust som undviks, direkt eller indirekt, genom överträdelsen,

f) graden av samarbete med nationella behöriga myndigheter för att komma till rätta med överträdelsen och minska dess potentiella negativa effekter,

g) operatörens grad av ansvar med beaktande av de tekniska och organisatoriska åtgärder som genomförts av denne,

h) det sätt på vilket överträdelsen kom till den nationella behöriga myndighetens kännedom, särskilt huruvida, och i sådana fall i vilken mån, operatören anmälde överträdelsen,

i) om överträdelsen skett med uppsåt eller genom oaktsamhet,

j) alla åtgärder som vidtagits av operatören för att minska den skada som de berörda personerna lidit.

8. Varje medlemsstat ska fastställa regler ▌ om i vilken utsträckning administrativa sanktionsavgifter får påföras offentliga myndigheter och organ som är inrättade i medlemsstaten.

9. Beroende på medlemsstatens rättssystem får reglerna om administrativa sanktionsavgifter tillämpas på ett sådant sätt att sanktionsavgifterna utdöms av behöriga nationella domstolar ***eller*** andra organ, beroende på vad som är tillämpligt i dessa medlemsstater. Tillämpningen av sådana regler i dessa medlemsstater ska ha motsvarande verkan.

10. Marknadskontrollmyndighetens utövande av sina befogenheter enligt denna artikel ska omfattas av lämpliga rättssäkerhetsgarantier i enlighet med unionsrätten och nationell rätt, inbegripet effektiva rättsmedel och rättssäkerhet.

11. Medlemsstaterna ska årligen underrätta kommissionen om de administrativa sanktionsavgifter som de har utfärdat under det året, i enlighet med denna artikel, och om eventuella relaterade rättstvister eller rättsliga förfaranden.

Artikel 100

Administrativa sanktionsavgifter för unionens institutioner, organ och byråer

1. Europeiska datatillsynsmannen får ålägga administrativa sanktionsavgifter för de av unionens institutioner, organ och byråer som omfattas av denna förordning. Vid beslut om huruvida administrativa sanktionsavgifter ska åläggas och beslut om storleken på den administrativa sanktionsavgiften i varje enskilt fall ska alla relevanta omständigheter i den specifika situationen beaktas och vederbörlig hänsyn ska tas till

a) överträdelsens art, svårighetsgrad och varaktighet samt dess konsekvenser, ***det berörda AI-systemets syfte samt antalet berörda personer och omfattningen av den skada som de har lidit och alla relevanta tidigare överträdelser,***

b) graden av unionsinstitutionens, unionsorganets eller unionsbyråns ansvar, med beaktande av de tekniska och organisatoriska åtgärder som de har genomfört,

c) alla åtgärder som unionsinstitutionen, unionsorganet eller unionsbyrån vidtar för att mildra den skada som de berörda personerna lidit,

d) ***graden av*** samarbete med Europeiska datatillsynsmannen för att åtgärda överträdelsen och minska dess potentiella negativa effekter, inbegripet efterlevnad av någon av de åtgärder som tidigare förordnats av Europeiska datatillsynsmannen mot unionens berörda institution, organ eller byrå med avseende på samma fråga,

e) eventuella liknande tidigare överträdelser som begåtts av unionens institution, organ eller byrå,

f) det sätt på vilket överträdelsen kom till Europeiska datatillsynsmannens kännedom, särskilt huruvida och i så fall i vilken omfattning unionsinstitutionen, unionsorganet eller unionsbyrån anmälde överträdelsen,

g) den årliga budgeten för unionsinstitutionen, unionsbyrån eller unionsorganet.

2. ***Bristande efterlevnad av det förbud mot AI-metoder som avses i artikel 5*** ska medföra administrativa sanktionsavgifter på upp till ***1 500 000 EUR.***

▌

3. AI-systemets bristande efterlevnad av andra krav eller skyldigheter enligt denna förordning än de som fastställs i artikel 5 ▌ ska medföra administrativa sanktionsavgifter på upp till ▌ ***750 000*** EUR.

4. Innan ett beslut fattas enligt denna artikel ska Europeiska datatillsynsmannen ge den eller det av unionens institutioner, organ eller byråer som är föremål för förfarandet som genomförs av Europeiska datatillsynsmannen möjlighet att höras om den möjliga överträdelsen. Europeiska datatillsynsmannen ska grunda sina beslut endast på inslag och omständigheter som de berörda parterna har getts möjlighet att yttra sig om. Eventuella klagande ska vara nära knutna till förfarandet.

5. De berörda parternas rätt till försvar ska iakttas fullständigt i förfarandena. De ska ha rätt att få tillgång till Europeiska datatillsynsmannens akt, med förbehåll för enskildas eller företags berättigade intresse av skydd av sina personuppgifter eller affärshemligheter.

6. De medel som samlats in genom åläggande av sanktionsavgifter i denna artikel ska ***bidra till unionens allmänna budget. Sanktionsavgifterna får inte påverka den ändamålsenliga funktionen för*** den unions***institution,*** det unions***organ eller*** unions***byrå som ålagts sanktionsavgiften.***

7. Europeiska datatillsynsmannen ska årligen underrätta kommissionen om de administrativa sanktionsavgifter som den ålagt i enlighet med denna artikel och om eventuella rättstvister eller rättsliga förfaranden den inlett.

Artikel 101

Sanktionsavgifter för leverantörer av AI-modeller för allmänna ändamål

1. Kommissionen får ålägga leverantörer av AI-modeller för allmänna ändamål sanktionsavgifter på upp till 3 % av deras totala globala omsättning under det föregående räkenskapsåret eller 15 miljoner euro, beroende på vilket som är högst, om kommissionen konstaterar att leverantören uppsåtligen eller av oaktsamhet

a) överträtt de relevanta bestämmelserna i denna förordning,

b) underlåtit att tillmötesgå en begäran om en handling eller om information enligt artikel 91, eller lämnat oriktiga, ofullständiga eller vilseledande uppgifter,

c) underlåtit att följa en åtgärd som begärts enligt artikel 93,

d) underlåtit att ge kommissionen tillgång till AI-modellen för allmänna ändamål eller AI-modellen för allmänna ändamål med systemrisk i syfte att genomföra en utvärdering i enlighet med artikel 92.

Vid fastställandet av sanktionsavgiften eller det löpande vitesbeloppet ska hänsyn tas till överträdelsens art, allvarlighet och varaktighet, varvid vederbörlig hänsyn ska tas till principerna om proportionalitet och lämplighet. Kommissionen ska också beakta åtaganden som gjorts i enlighet med artikel 93.3 eller som gjorts i relevanta uppförandekoder i enlighet med artikel 56.

2. Innan kommissionen antar beslutet enligt punkt 1 ska den meddela sina preliminära iakttagelser till leverantören av AI-modellen för allmänna ändamål eller AI-modellen för allmänna ändamål med systemrisk och ge denne möjlighet att höras.

3. Sanktionsavgifter som åläggs i enlighet med denna artikel ska vara effektiva, proportionella och avskräckande.

4. Information om sanktionsavgifter som ålagts enligt denna artikel ska också lämnas till nämnden när så är lämpligt.

5. Europeiska unionens domstol ska ha obegränsad behörighet att pröva kommissionens beslut om fastställande av sanktionsavgifter enligt denna artikel. Den får upphäva, sänka eller höja ålagda sanktionsavgifter.

6. Kommissionen ska anta genomförandeakter med närmare bestämmelser för förfaranden inför ett eventuellt antagande av beslut enligt punkt 1 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

KAPITEL XIII
SLUTBESTÄMMELSER

Artikel 102

Ändring av förordning (EG) nr 300/2008

I artikel 4.3 i förordning (EG) nr 300/2008 ska följande stycke läggas till:

” Vid antagandet av detaljerade bestämmelser avseende tekniska specifikationer och förfaranden för godkännande och användning av säkerhetsutrustning som rör system för artificiell intelligens i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/ ... * [+], ska kraven i avdelning III kapitel 2 i den förordningen beaktas.

---

* Europaparlamentets och rådets förordning (EU) 2024/ ... om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter (EUT L, ELI: ...).”.

[+] EUT: för in i texten numret på denna förordning (2021/0106(COD)) och komplettera motsvarande fotnot.

Artikel 103

Ändring av förordning (EU) nr 167/2013

I artikel 17.5 i förordning (EU) nr 167/2013 ska följande stycke läggas till:

”Vid antagandet av delegerade akter i enlighet med det första stycket rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/ ... *[+] ska kraven i avdelning III kapitel 2 i den förordningen beaktas.

---

* Europaparlamentets och rådets förordning (EU) 2024/ ... om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter (EUT L, ELI: ...)”.

+ EUT: för in i texten numret på denna förordning (2021/0106(COD)) och komplettera motsvarande fotnot.

Artikel 104

Ändring av förordning (EU) nr 168/2013

I artikel 22.5 i förordning (EU) nr 168/2013 ska följande stycke läggas till:

”Vid antagandet av delegerade akter i enlighet med det första stycket rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/ ... *[+] ska kraven i avdelning III kapitel 2 i den förordningen beaktas.

---

[*] Europaparlamentets och rådets förordning (EU) 2024/ ... om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter (EUT L, ELI: ...)”.

[+] EUT: för in i texten numret på denna förordning (2021/0106(COD)) och komplettera motsvarande fotnot.

Artikel 105

Ändring av direktiv 2014/90/EU

I artikel 8 i direktiv 2014/90/EU ska följande punkt läggas till:

” 5. För system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/ ... [+]* ska kommissionen, när den utför sin verksamhet i enlighet med punkt 1 och när den antar tekniska specifikationer och provningsstandarder i enlighet med punkterna 2 och 3, beakta de krav som anges i avdelning III kapitel 2 i den förordningen.

---

* Europaparlamentets och rådets förordning (EU) 2024/ ... om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter (EUT L, ELI: ...)”.

+ EUT: för in i texten numret på denna förordning (2021/0106(COD)) och komplettera motsvarande fotnot.

Artikel 106

Ändring av direktiv (EU) 2016/797

I artikel 5 i direktiv (EU) 2016/797 ska följande punkt läggas till:

” 12. Vid antagandet av delegerade akter i enlighet med punkt 1 och genomförandeakter i enlighet med punkt 11 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/ ...[+] * ska kraven i avdelning III kapitel 2 i den förordningen beaktas.

---

* Europaparlamentets och rådets förordning (EU) 2024/ ... om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter (EUT L, ELI: ...)”.

[+] EUT: för in i texten numret på denna förordning (2021/0106(COD)) och komplettera motsvarande fotnot.

Artikel 107

Ändring av förordning (EU) 2018/858

I artikel 5 i förordning (EU) 2018/858 ska följande punkt läggas till:

” 4. Vid antagandet av delegerade akter i enlighet med punkt 3 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/ ... *[+] ska kraven i avdelning III kapitel 2 i den förordningen beaktas.

---

* Europaparlamentets och rådets förordning (EU) 2024/ ... om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter (EUT L, ELI: ...)”.

+ EUT: för in i texten numret på denna förordning (2021/0106(COD)) och komplettera motsvarande fotnot.

Artikel 108

Ändring av förordning (EU) 2018/1139

Förordning (EU) 2018/1139 ska ändras på följande sätt:

1. I artikel 17 ska följande punkt läggas till:

” 3. Utan att det påverkar tillämpningen av punkt 2 ska vid antagandet av genomförandeakter i enlighet med punkt 1 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/ ... *[+] kraven i avdelning III kapitel 2 i den förordningen beaktas.

---

* Europaparlamentets och rådets förordning (EU) 2024/ ... om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter (EUT L, ELI: ...)”.

2. I artikel 19 ska följande punkt läggas till:

” 4. Vid antagandet av delegerade akter i enlighet med punkterna 1 och 2 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i förordning (EU) 2024/ ... [++] ska kraven i avdelning III kapitel 2 i den förordningen beaktas.”.

[+] EUT: för in i texten numret på denna förordning (2021/0106(COD)) och komplettera motsvarande fotnot.

[++] EUT: för in numret på denna förordning i (2021/0106 (COD)).

3. I artikel 43 ska följande punkt läggas till:

” 4. Vid antagandet av genomförandeakter i enlighet med punkt 1 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i förordning (EU) 2024/ ... [+] ska kraven i avdelning III kapitel 2 i den förordningen beaktas.”.

4. I artikel 47 ska följande punkt läggas till:

” 3. Vid antagandet av delegerade akter i enlighet med punkterna 1 och 2 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i förordning (EU) 2024/ ... [+] ska kraven i avdelning III kapitel 2 i den förordningen beaktas.”.

5. I artikel 57 ska följande punkt läggas till:

”Vid antagandet av dessa genomförandeakter rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i förordning (EU) 2024/ ... [+] ska kraven i avdelning III kapitel 2 i den förordningen beaktas.”.

[+] EUT: för in numret på denna förordning i (2021/0106 (COD)).

6. I artikel 58 ska följande punkt läggas till:

” 3. Vid antagandet av delegerade akter i enlighet med punkterna 1 och 2 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i förordning (EU) 2024/ ... [+] ska kraven i avdelning III kapitel 2 i den förordningen beaktas.”.

Artikel 109

Ändring av förordning (EU) 2019/2144

I artikel 11 i förordning (EU) 2019/2144 ska följande punkt läggas till:

” 3. Vid antagandet av genomförandeakter i enlighet med punkt 2 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/ ... *[++] ska kraven i avdelning III kapitel 2 i den förordningen beaktas.

---

* Europaparlamentets och rådets förordning 2024/ ... om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter (EUT L, ELI: ...)”.

[+] EUT: för in numret på denna förordning i (2021/0106 (COD)).

[++] EUT: för in i texten numret på denna förordning (2021/0106(COD)) och komplettera motsvarande fotnot.

Artikel 110

Ändring av direktiv (EU) 2020/1828

I bilaga I till Europaparlamentets och rådets direktiv (EU) 2020/1828*[61] *ska följande punkt läggas till:

” ***68.*** ***Europaparlamentets och rådets*** förordning ***(EU) 2024/… om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter (EUT L, ELI: …)”.***

[61] Europaparlamentets och rådets direktiv (EU) 2020/1828 av den 25 november 2020 om grupptalan för att skydda konsumenters kollektiva intressen och om upphävande av direktiv 2009/22/EG (EUT L 409, 4.12.2020, s. 1).

Artikel 111

AI-system som redan släppts ut på marknaden eller tagits i bruk

1. ***Utan att det påverkar tillämpningen av artikel 5 enligt artikel*** 113.3 a ***ska*** AI-system som är komponenter i de stora it-system som inrättats genom de rättsakter som förtecknas i bilaga X och som har släppts ut på marknaden eller tagits i bruk före ▌ den ... [36 månader efter dagen för denna förordnings ikraftträdande] ***bringas i överensstämmelse med denna förordning senast den 31 december 2030.***

   De krav som fastställs i denna förordning ska beaktas ▌ vid den utvärdering av varje stort it-system inrättat genom de rättsakter förtecknade i bilaga X som ska utföras i enlighet med de rättsakterna och i de fall ***dessa rättsakter ersätts eller ändras.***

2. ***Utan att det påverkar tillämpningen av artikel 5 enligt artikel*** 113.3 a ska denna förordning tillämpas på andra ***operatörer av*** AI-system med hög risk än de system som avses i punkt 1 i den här artikeln och som har släppts ut på marknaden eller tagits i bruk före den... [24 månader efter dagen för denna förordnings ikraftträdande], endast om dessa system från och med den dagen förändras betydligt när det gäller sin ***utformning***. ***När det gäller AI-system med hög risk*** som är avsedda ***att användas av offentliga myndigheter ska leverantörer och spridare av sådana system vidta nödvändiga åtgärder för att uppfylla kraven i denna förordning senast den ... [sex år efter dagen för denna förordnings ikraftträdande].***

3. Leverantörer av AI-modeller för allmänna ändamål som har släppts ut på marknaden före den... [***12*** månader efter dagen för denna förordnings ikraftträdande***] ska vidta nödvändiga åtgärder för att uppfylla de skyldigheter som fastställs i denna förordning senast den... [36 månader*** efter dagen för denna förordnings ikraftträdande***].***

Artikel 112

Utvärdering och översyn

1. Kommissionen ska bedöma behovet av att ändra förteckningen i bilaga III ***och av förteckningen i artikel 5 över förbjudna AI-metoder*** en gång om året efter det att denna förordning har trätt i kraft ***och fram till utgången av perioden för delegering av befogenhet i artikel 97. Kommissionen ska lägga fram resultaten av denna bedömning för Europaparlamentet och rådet.***

2. ***Senast den... [fyra år efter dagen för denna förordnings ikraftträdande] och därefter vart fjärde år ska kommissionen utvärdera och rapportera till Europaparlamentet och rådet om följande:***

   a) Behovet av ändringar som utvidgar befintliga områdesrubriker eller lägger till nya områdesrubriker i bilaga III.

   b) Ändringar av förteckningen över AI-system som kräver ytterligare transparensåtgärder i enlighet med artikel 50.

   c) Ändringar som ökar tillsyns- och styrningssystemets effektivitet.

3. Kommissionen ska ***senast den*** ... ***[***fyra år efter dagen för denna förordnings ikraftträdande] och därefter vart fjärde år överlämna en rapport om utvärderingen och översynen av denna förordning till Europaparlamentet och rådet. ***Rapporten ska innehålla en bedömning av efterlevnadsstrukturen och det eventuella behovet av att en unionsbyrå åtgärdar eventuella konstaterade brister. På grundval av resultaten ska denna rapport vid behov åtföljas av ett förslag till ändring av denna förordning.*** Rapporten ska offentliggöras.

4. I de rapporter som avses i punkt 2 ska särskild uppmärksamhet ägnas åt

   a) statusen för de nationella behöriga myndigheternas ekonomiska resurser, ***tekniska*** utrustning och personal för att effektivt kunna utföra de uppgifter som de tilldelas enligt denna förordning,

   b) tillståndet för sanktionerna, särskilt de administrativa sanktionsavgifter som avses i artikel 99.1 och som tillämpas av medlemsstaterna på överträdelser av bestämmelserna i denna förordning,

c) antagna harmoniserade standarder och gemensamma specifikationer som utarbetats till stöd för denna förordning,

d) antalet företag som kommer in på marknaden efter det att denna förordning har börjat tillämpas och hur många av dem som är små och medelstora företag.

5. Senast den... [fyra år efter dagen för denna förordnings ikraftträdande] ska kommissionen utvärdera AI-byråns funktion, huruvida byrån har fått tillräckliga befogenheter och tillräcklig behörighet för att fullgöra sina uppgifter och huruvida det skulle vara relevant och nödvändigt för ett korrekt genomförande och en korrekt efterlevnad av denna förordning att uppgradera byrån och dess befogenheter när det gäller efterlevnadskontroll och öka dess resurser. Kommissionen ska överlämna denna utvärderingsrapport till Europaparlamentet och rådet.

6. Senast den... [fyra år efter dagen för denna förordnings ikraftträdande] och därefter vart fjärde år ska kommissionen lägga fram en rapport om översynen av framstegen med utvecklingen av standardiseringsprodukter för energieffektiv utveckling av AI-modeller för allmänna ändamål, och utvärdera behovet av ytterligare åtgärder eller insatser, inbegripet bindande åtgärder eller insatser . Rapporten ska överlämnas till Europaparlamentet och rådet, och den ska offentliggöras.

7. Senast den **…** [***fyra år*** efter den här förordningens ikraftträdande] och därefter vart ***tredje*** år ska kommissionen utvärdera de ***frivilliga*** uppförandekodernas inverkan och effektivitet för att främja tillämpningen av kraven i kapitel II avsnitt 2 ***för andra AI-system än AI-system med hög risk*** och eventuellt andra ytterligare krav för AI-system andra än AI-system med hög risk***, inbegripet vad gäller miljömässig hållbarhet.***

8. Vid tillämpning av punkterna 1–7 ska nämnden, medlemsstaterna och de nationella behöriga myndigheterna vid begäran tillhandahålla information till kommissionen ***utan onödigt dröjsmål.***

9. Kommissionen ska när den utför de utvärderingar och översyner som avses i punkterna 1 till 7 ta hänsyn till ståndpunkter och slutsatser från nämnden, Europaparlamentet, rådet och andra relevanta organ eller källor.

10. Kommissionen ska om nödvändigt överlämna lämpliga förslag om ändring av denna förordning, med särskild hänsyn till teknikens utveckling ***och AI-systems inverkan på hälsa och säkerhet och grundläggande rättigheter*** och mot bakgrund av tendenserna inom informationssamhället.

11. För att vägleda de utvärderingar och översyner som avses i punkterna 1–7 ska AI-byrån åta sig att ta fram en objektiv och deltagandebaserad metod för utvärdering av risknivåerna på grundval av de kriterier som anges i de relevanta artiklarna och införandet av nya system i

a) förteckningen i bilaga III, inbegripet utvidgning av befintliga områdesrubriker eller tillägg av nya områdesrubriker i denna bilaga,

b) förteckningen över de förbjudna metoder som fastställs i artikel 5 och

c) förteckningen över AI-system som kräver ytterligare transparensåtgärder i enlighet med artikel 50.

12. Varje ändring av denna förordning enligt punkt 10, eller relevanta delegerade akter eller genomförandeakter, som rör den sektorsspecifika unionslagstiftning om harmonisering som förtecknas i bilaga I avsnitt B, ska ta hänsyn till särdragen i lagstiftningen inom varje sektor och befintliga styrnings-, överensstämmelsebedömnings- och efterlevnadsmekanismer och myndigheter som inrättats i denna.

13. Senast ... [sju år efter ikraftträdandet av denna förordning] ska kommissionen göra en bedömning av efterlevnaden av denna förordning och lämna en rapport om detta till Europaparlamentet, rådet samt Europeiska ekonomiska och sociala kommittén med beaktande av de första åren av tillämpningen av denna förordning. På grundval av resultaten ska denna rapport vid behov åtföljas av ett förslag till ändring av denna förordning med avseende på efterlevnadsstrukturen och behovet av att en EU-byrå åtgärdar eventuella konstaterade brister.

Artikel 113

Ikraftträdande och tillämpning

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Den ska tillämpas från och med den ... [24 månader efter dagen för denna förordnings ikraftträdande].

Emellertid gäller att

▌

a) kapitel I och II ska tillämpas från och med den ... [sex månader efter dagen för denna förordnings ikraftträdande], att

b) kapitel III ▌ avsnitt 4***,*** kapitel V, kapitel VII ***och kapitel XII*** ska tillämpas från och med den ... [***12*** månader efter dagen för denna förordnings ikraftträdande], ***med undantag för artikel 101,*** och att

c) artikel 6.1 ***och motsvarande krav i denna förordning*** ska tillämpas från och med den … [***36*** månader från dagen för denna förordnings ikraftträdande].

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i ...

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

BILAGA I

Förteckning över unionslagstiftning om harmonisering

Avsnitt A – Förteckning över unionslagstiftning om harmonisering som bygger på den nya lagstiftningsramen

1. Europaparlamentets och rådets direktiv 2006/42/EG av den 17 maj 2006 om maskiner och om ändring av direktiv 95/16/EG (EUT L 157, 9.6.2006, s. 24) [upphävt genom maskinförordningen].

2. Europaparlamentets och rådets direktiv 2009/48/EG av den 18 juni 2009 om leksakers säkerhet (EUT L 170, 30.6.2009, s. 1).

3. Europaparlamentets och rådets direktiv 2013/53/EU av den 20 november 2013 om fritidsbåtar och vattenskotrar och om upphävande av direktiv 94/25/EG (EUT L 354, 28.12.2013, s. 90).

4. Europaparlamentets och rådets direktiv 2014/33/EU av den 26 februari 2014 om harmonisering av medlemsstaternas lagstiftning om hissar och säkerhetskomponenter till hissar (EUT L 96, 29.3.2014, s. 251).

5. Europaparlamentets och rådets direktiv 2014/34/EU av den 26 februari 2014 om harmonisering av medlemsstaternas lagstiftning om utrustning och skyddssystem som är avsedda för användning i potentiellt explosiva atmosfärer (EUT L 96, 29.3.2014, s. 309).

6. Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG (EUT L 153, 22.5.2014, s. 62).

7. Europaparlamentets och rådets direktiv 2014/68/EU av den 15 maj 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av tryckbärande anordningar (EUT L 189, 27.6.2014, s. 164).

8. Europaparlamentets och rådets förordning (EU) 2016/424 av den 9 mars 2016 om linbaneanläggningar och om upphävande av direktiv 2000/9/EG (EUT L 81, 31.3.2016, s. 1).

9. Europaparlamentets och rådets förordning (EU) 2016/425 av den 9 mars 2016 om personlig skyddsutrustning och om upphävande av rådets direktiv 89/686/EEG (EUT L 81, 31.3.2016, s. 51).

10. Europaparlamentets och rådets förordning (EU) 2016/426 av den 9 mars 2016 om anordningar för förbränning av gasformiga bränslen och om upphävande av direktiv 2009/142/EG (EUT L 81, 31.3.2016, s. 99).

11. Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, om ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG (EUT L 117, 5.5.2017, s. 1).

12. Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för in vitro-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU (EUT L 117, 5.5.2017, s. 176).

Avsnitt B. Förteckning över annan unionslagstiftning om harmonisering

13. Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002 (EUT L 97, 9.4.2008, s. 72).

14. Europaparlamentets och rådets förordning (EU) nr 168/2013 av den 15 januari 2013 om godkännande av och marknadstillsyn för två- och trehjuliga fordon och fyrhjulingar (EUT L 60, 2.3.2013, s. 52).

15. Europaparlamentets och rådets förordning (EU) nr 167/2013 av den 5 februari 2013 om godkännande och marknadstillsyn av jordbruks- och skogsbruksfordon (EUT L 60, 2.3.2013, s. 1).

16. Europaparlamentets och rådets direktiv 2014/90/EU av den 23 juli 2014 om marin utrustning och om upphävande av rådets direktiv 96/98/EG (EUT L 257, 28.8.2014, s. 146).

17. Europaparlamentets och rådets direktiv (EU) 2016/797 av den 11 maj 2016 om driftskompatibiliteten hos järnvägssystemet inom Europeiska unionen (EUT L 138, 26.5.2016, s. 44).

18. Europaparlamentets och rådets förordning (EU) 2018/858 av den 30 maj 2018 om godkännande av och marknadskontroll över motorfordon och släpfordon till dessa fordon samt av system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, om ändring av förordningarna (EG) nr 715/2007 och (EG) nr 595/2009 samt om upphävande av direktiv 2007/46/EG (EUT L 151, 14.6.2018, s. 1).

19. Europaparlamentets och rådets förordning (EU) 2019/2144 av den 27 november 2019 om krav för typgodkännande av motorfordon och deras släpvagnar samt de system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, med avseende på deras allmänna säkerhet och skydd för personer i fordonet och oskyddade trafikanter, om ändring av Europaparlamentets och rådets förordning (EU) 2018/858 och om upphävande av Europaparlamentets och rådets förordningar (EG) nr 78/2009, (EG) nr 79/2009 och (EG) nr 661/2009 samt kommissionens förordningar (EG) nr 631/2009, (EU) nr 406/2010, (EU) nr 672/2010, (EU) nr 1003/2010, (EU) nr 1005/2010, (EU) nr 1008/2010, (EU) nr 1009/2010, (EU) nr 19/2011, (EU) nr 109/2011, (EU) nr 458/2011, (EU) nr 65/2012, (EU) nr 130/2012, (EU) nr 347/2012, (EU) nr 351/2012, (EU) nr 1230/2012 och (EU) 2015/166 (EUT L 325, 16.12.2019, s. 1).

20. Europaparlamentets och rådets förordning (EU) nr 2018/1139 av den 4 juli 2018 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 2111/2005, (EG) nr 1008/2008, (EU) nr 996/2010, (EU) nr 376/2014 och direktiv 2014/30/EU och 2014/53/EU, samt om upphävande av Europaparlamentets och rådets förordningar (EG) nr 552/2004 och (EG) nr 216/2008 och rådets förordning (EEG) nr 3922/91 (EUT L 212, 22.8.2018, s. 1), i den mån det rör sig om konstruktion, produktion och utsläppande på marknaden av luftfartyg som avses i artikel 2.1 a och b i den förordningen, när det gäller obemannade luftfartyg och deras motorer, propellrar, delar och utrustning för att kontrollera dem på distans.

BILAGA II

Förteckning över de brott som avses i artikel 5.1 e iii

Brott som avses i artikel 5.1 e iii:

– ***Terrorism.***

– ***Människohandel.***

– ***Sexuell exploatering av barn och barnpornografi.***

– ***Olaglig handel med narkotika och psykotropa ämnen.***

– ***Olaglig handel med vapen, ammunition och sprängämnen.***

– ***Mord och grov misshandel.***

– ***Olaglig handel med mänskliga organ eller vävnader.***

– ***Olaglig handel med nukleära och radioaktiva ämnen.***

– ***Människorov, olaga frihetsberövande och tagande av gisslan.***

– *Brott som omfattas av Internationella brottmålsdomstolens jurisdiktion.*

– *Olagligt beslagtagande av ett flygplan eller ett fartyg.*

– *Våldtäkt.*

– *Miljöbrott.*

– *Organiserad stöld eller väpnat rån.*

– *Sabotage.*

– *Deltagande i en kriminell organisation inblandad i ett eller flera av de brott som förtecknas ovan.*

BILAGA III

AI-system med hög risk som avses i artikel 6.2

AI-system med hög risk enligt artikel 6.2 är de AI-system som används inom något av följande områden:

1. ***Biometri, i den mån användningen är tillåten enligt relevant unionsrätt eller nationell rätt:***

   a) ***System för biometrisk fjärridentifiering.***

   Detta ska inte omfatta de AI-system som är avsedda att användas för ***biometrisk verifiering och vars enda syfte är att bekräfta att en viss*** fysisk ***person är den person som han eller hon påstår sig vara.***

   b) AI-system som är avsedda att användas för biometrisk kategorisering enligt känsliga eller skyddade attribut eller egenskaper som grundar sig på inferens av dessa attribut eller egenskaper.

   c) AI-system som är avsedda att användas för känsloigenkänning.

2. ▌Kritisk infrastruktur:

   a) AI-system som är avsedda att användas som säkerhetskomponenter i samband med förvaltning och drift av ***kritisk digital infrastruktur***, vägtrafik eller i samband med tillhandahållande av vatten, gas, värme och el.

3. Utbildning och yrkesutbildning:

   a) AI-system som är avsedda att användas ***för att fastställa tillgång eller antagande eller för att anvisa*** fysiska personer till institutioner för yrkesutbildning eller annan utbildning ***på alla nivåer.***

   b) AI-system som är avsedda att användas ***för att utvärdera läranderesultat, även när dessa resultat används för att styra fysiska personers inlärningsprocess vid institutioner för yrkesutbildning eller annan utbildning på alla nivåer.***

   c) AI-system som är avsedda att användas för att bedöma den lämpliga utbildningsnivå som en person kommer att erhålla eller kommer att kunna få tillgång till, inom ramen för eller vid utbildnings- och yrkesutbildningsinstitutioner.

   d) AI-system som är avsedda att användas för att övervaka och upptäcka förbjudet beteende bland studenterna under provtillfällen inom ramen för eller vid utbildnings- och yrkesutbildningsinstitutioner.

4. Sysselsättning, arbetsledning och tillgång till egenföretagande:

   a) AI-system som är avsedda att användas för rekrytering eller urval av fysiska personer, särskilt för ***att publicera riktade platsannonser, analysera och filtrera platsansökningar och utvärdera kandidater.***

   b) AI-system som är avsedd att användas ***för att fatta*** beslut ***som påverkar villkoren för arbetsrelaterade förhållanden,*** befordringar och uppsägningar av arbetsrelaterade avtalsförhållanden, ***för uppgiftsfördelning på grundval av individuellt beteende eller personlighetsdrag eller egenskaper eller för att övervaka och utvärdera*** personers prestationer och beteende inom ramen för sådana förhållanden.

5. Tillgång till och åtnjutande av grundläggande privata tjänster och ***väsentliga*** offentliga tjänster och förmåner:

   a) AI-system som är avsedda att användas av offentliga myndigheter eller för offentliga myndigheters räkning för att utvärdera fysiska personers rätt till ***väsentliga*** förmåner och ***tjänster*** i form av offentligt stöd***, inbegripet hälso- och sjukvårdstjänster,*** samt för att bevilja, minska, upphäva eller återkalla sådana förmåner och tjänster.

   b) AI-system som är avsedda att användas för att utvärdera fysiska personers kreditvärdighet eller fastställa deras kreditbetyg, med undantag för AI-system ***som används i syfte att upptäcka ekonomiska bedrägerier.***

c) ***AI-system som är avsedda att användas för riskbedömning och prissättning i förhållande till fysiska personer när det gäller livförsäkring och sjukförsäkring.***

d) AI-system som är avsedda att ***utvärdera och klassificera nödsamtal från fysiska personer eller*** användas för att sända ut eller för att fastställa prioriteringsordningen för utsändning av larmtjänster, inbegripet ***polis,*** brandkår och ambulans***, samt av patientsorteringssystem för akutsjukvård.***

6. Brottsbekämpning***, i den mån användningen är tillåten enligt relevant unionsrätt eller nationell rätt:***

a) AI-system som är avsedda att användas av brottsbekämpande myndigheter***, eller på brottsbekämpande myndigheters vägnar, eller av unionens institutioner, organ, kontor eller byråer*** för att bedöma risken för att en fysisk person ***blir ett offer för*** brott.

b) AI-system som är avsedda att användas av brottsbekämpande myndigheter***, eller på brottsbekämpande myndigheters vägnar, eller av unionens institutioner, organ, kontor eller byråer till stöd för brottsbekämpande myndigheter, såsom lögndetektorer eller liknande verktyg.***

▌

c) AI-system som är avsedda att användas av brottsbekämpande myndigheter***, eller på brottsbekämpande myndigheters vägnar, eller av unionens institutioner, organ, kontor eller byråer till stöd för brottsbekämpande myndigheter för att bedöma*** hur pass tillförlitlig bevisningen är i samband med utredning eller lagföring av brott.

d) AI-system som är avsedda att användas av brottsbekämpande myndigheter***, eller på brottsbekämpande myndigheters vägnar, eller av unionens institutioner, organ, kontor eller byråer till stöd för brottsbekämpande myndigheter för att bedöma sannolikheten för att en fysisk person begår eller på nytt begår ett brott, ej enbart*** baserat på profilering av fysiska personer i enlighet med artikel 3.4 i direktiv (EU) 2016/680 eller ***för att bedöma*** fysiska personers eller gruppers personlighetsdrag och egenskaper eller tidigare brottsliga beteende.

e) AI-system som är avsedda att användas av brottsbekämpande myndigheter***, eller på brottsbekämpande myndigheters vägnar, eller av unionens institutioner, organ, kontor eller byråer till stöd för*** brottsbekämpande myndigheter för profilering av fysiska personer enligt artikel 3.4 i direktiv (EU) 2016/680 vid upptäckt, utredning eller lagföring av brott.

7. Migration, asyl och gränskontrollförvaltning***, i den mån användningen är tillåten enligt relevant unionsrätt eller nationell rätt:***

a) AI-system som är avsedda att användas av behöriga myndigheter, såsom lögndetektorer och liknande verktyg***.***

b) AI-system som är avsedda att användas av brottsbekämpande myndigheter***, eller på brottsbekämpande myndigheters vägnar, eller av unionens institutioner, organ, kontor eller byråer*** för att bedöma en risk, inbegripet en säkerhetsrisk, en risk för irreguljär ***migration*** eller en hälsorisk som utgörs av en fysisk person som avser resa in på eller har rest in på en medlemsstats territorium.

c) AI-system som är avsedda att användas av brottsbekämpande myndigheter***, eller på brottsbekämpande myndigheters vägnar, eller av unionens institutioner, organ, kontor eller byråer*** för att bistå behöriga offentliga myndigheter vid prövningen av ansökningar om asyl, visering eller uppehållstillstånd och för därmed sammanhängande klagomål om huruvida de fysiska personer som ansöker om status uppfyller kraven***, inbegripet relaterade bedömningar av bevisens tillförlitlighet.***

d) AI-system som är avsedda att användas av behöriga offentliga myndigheter, inbegripet unionens institutioner, organ, kontor eller byråer, eller på deras vägnar, i samband med migrations-, asyl- eller gränskontrollförvaltning, i syfte att upptäcka, känna igen eller identifiera fysiska personer, med undantag för verifiering av resehandlingar.

8. Rättskipning och demokratiska processer:

a) AI-system som är avsedda ***att användas av en rättslig myndighet eller på dess vägnar för att*** hjälpa en rättslig myndighet att undersöka och tolka fakta och lagstiftning och att tillämpa lagen på konkreta fakta ***eller som är avsedda att användas på ett likande sätt i alternativa tvistlösningar.***

b) ***AI-system som är avsedda att användas för att påverka resultatet av ett val eller en folkomröstning eller fysiska personers röstningsbeteende när dessa utövar sin rätt att rösta i val eller folkomröstningar. Detta omfattar inte AI-system vars utdata fysiska personer inte är direkt exponerade för, såsom verktyg som används för att organisera, optimera eller strukturera politiska kampanjer ur administrativ eller logistisk synvinkel.***

BILAGA IV

Teknisk dokumentation som avses i artikel 11.1

Den tekniska dokumentation som avses i artikel 11.1 ska minst innehålla följande information, beroende på vad som är tillämpligt för det relevanta AI-systemet:

1. En allmän beskrivning av AI-systemet, inklusive

   a) det avsedda syftet, ***namnet på leverantören*** och version av systemet, s***om återspeglar dess samband med tidigare versioner***,

   b) hur AI-systemet interagerar eller kan användas för att interagera med maskinvara eller programvara, ***inbegripet med andra AI-system som*** inte ingår i själva AI-systemet, i tillämpliga fall,

   c) versioner av relevant programvara eller fast programvara och eventuella krav med koppling till uppdatering av versioner,

   d) en beskrivning av alla format i vilka AI-systemet släpps ut på marknaden eller tas i bruk***, t.ex. programvarupaket inbäddat i maskinvara, nedladdningar eller API,***

e) en beskrivning av den maskinvara som AI-systemet är avsett att köras på,

f) om AI-systemet är en produktkomponent, fotografier eller illustrationer där de yttre egenskaperna framgår, samt dessa produkters märkning och interna utformning,

g) en grundläggande beskrivning av det användargränssnitt som tillhandahålls spridaren,

h) bruksanvisningar ***för spridaren och,*** i tillämpliga fall ***, en grundläggande beskrivning av det användargränssnitt som tillhandahålls spridaren***.

2. En utförlig beskrivning av komponenterna i AI-systemet och av processen för utveckling av detta, inklusive

a) de metoder och åtgärder som vidtas för att utveckla AI-systemet, inbegripet, i relevanta fall, användningen av förtränade system eller verktyg som tillhandahålls av tredje part och hur dessa har använts, integrerats eller ändrats av leverantören,

b) systemets designspecifikationer, dvs. AI-systemets och algoritmernas allmänna logik, de viktigaste valen vid utformningen, bl.a. motiveringen och de antaganden som gjorts, inbegripet med avseende på de personer eller grupper av personer som systemet är avsett att användas för, de viktigaste klassificeringsvalen, vad systemet har utformats för att optimera och de olika parametrarnas relevans, ***beskrivningen av systemets förväntade utdata och utdatakvalitet, de*** beslut om eventuella avvägningar mellan de tekniska lösningarna som valts för att uppfylla kraven i kapitel III avsnitt 2,

c) en beskrivning av systemarkitekturen som förklarar hur programvarukomponenter bygger på eller påverkar varandra och integreras i den övergripande behandlingen, de dataresurser som används för att utveckla, träna, testa och validera AI-systemet,

d) i relevanta fall uppgiftskraven i form av datablad som beskriver de träningsmetoder och träningstekniker och de träningsdataset som används, inbegripet ***en allmän beskrivning av dessa*** dataset, ***information om*** var dessa ***kommer från,*** deras omfattning och huvudsakliga egenskaper, hur uppgifterna inhämtades och valdes ut, märkningsförfaranden (t.ex. för övervakad inlärning), datarensningsmetoder (t.ex. upptäckt av avvikande värden),

e) en bedömning av de åtgärder för mänsklig tillsyn som krävs i enlighet med artikel 14, inbegripet en bedömning av de tekniska åtgärder som krävs för att underlätta ***spridarnas*** tolkning av AI-systemens resultat, i enlighet med artikel 13.3 d,

f) i tillämpliga fall, en utförlig beskrivning av sådana ändringar av AI-systemet och dess prestanda som fastställts på förhand, tillsammans med all relevant information om de tekniska lösningar som har valts för att säkerställa att AI-systemet kontinuerligt uppfyller de relevanta kraven i kapitel III avsnitt 2,

g) de validerings- och testningsförfaranden som används, inklusive information om de validerings- och testdata som har använts och deras huvudsakliga egenskaper, mått som används för att mäta noggrannhet, robusthet ▌ och överensstämmelse med andra relevanta krav som anges i kapitel III avsnitt 2 samt potentiellt diskriminerande effekter; testloggar och alla testrapporter, daterade och undertecknade av de ansvariga personerna, även med avseende på de på förhand fastställda ändringar som avses i led f.

h) de cybersäkerhetsåtgärder som vidtagits.

3. Detaljerade uppgifter om övervakning, drift och kontroll av AI-systemet, särskilt med avseende på dess kapacitet och prestandabegränsningar, inbegripet graden av noggrannhet för specifika personer eller grupper av personer som systemet är avsett att användas för och den övergripande förväntade noggrannhetsnivån i förhållande till det avsedda ändamålet, de förutsebara oavsiktliga resultaten och källorna till risker för hälsa och säkerhet, grundläggande rättigheter och diskriminering med tanke på AI-systemets avsedda ändamål, de åtgärder för mänsklig tillsyn som krävs i enlighet med artikel 14, inbegripet de tekniska åtgärder som har vidtagits för att underlätta ***spridarnas*** tolkning av AI-systemens resultat; specifikationerna av indata, beroende på vad som är lämpligt.

4. En beskrivning av lämpligheten hos resultatmåtten för det specifika AI-systemet.

5. En utförlig beskrivning av riskhanteringssystemet i enlighet med artikel 9.

6. En beskrivning av ***relevanta ändringar av systemet som görs av leverantören*** under dess livscykel.

7. En förteckning över de harmoniserade standarder som helt eller delvis tillämpas och som det hänvisas till i *Europeiska unionens officiella tidning*; om inga sådana harmoniserade standarder har tillämpats, en utförlig beskrivning av de lösningar som har valts för att uppfylla kraven i kapitel III avsnitt 2, inklusive en förteckning över andra relevanta standarder och tekniska specifikationer som har tillämpats.

8. En kopia av EU-försäkran om överensstämmelse.

9. En utförlig beskrivning av det system som har inrättats för att utvärdera AI-systemets prestanda efter det att systemet har släppts ut på marknaden i enlighet med artikel 72, inklusive den plan för övervakning efter utsläppande på marknaden som avses i artikel 72.3.

BILAGA V

EU-försäkran om överensstämmelse

Den EU-försäkran om överensstämmelse som avses i artikel 47 ska innehålla samtliga följande uppgifter:

1. AI-systemets namn och typ och eventuella ytterligare entydiga hänvisningar som gör det möjligt att identifiera och spåra AI-systemet.

2. Namn på och adress till leverantören eller, i förekommande fall, dennes ombud.

3. En uppgift om att EU-försäkran om överensstämmelse utfärdas på leverantörens eget ansvar.

4. En uppgift om att AI-systemet överensstämmer med denna förordning och, i tillämpliga fall, med annan relevant unionsrätt som föreskriver att en EU-försäkran om överensstämmelse ska utfärdas.

5. För AI-system som inbegriper behandling av personuppgifter, en förklaring om att AI-systemen i fråga uppfyller kraven i förordningarna (EU) 2016/679 och (EU) 2018/1725 och direktiv (EU) 2016/680.

6. Hänvisningar till relevanta harmoniserade standarder som används eller till andra gemensamma specifikationer för vilka överensstämmelse deklareras.

7. I tillämpliga fall, det anmälda organets namn och identifikationsnummer, en beskrivning av det förfarande för bedömning av överensstämmelse som har genomförts och uppgifter om det utfärdade intyget.

8. Ort och datum för utfärdande av försäkran, namn på och befattning för den person som undertecknade den, uppgift om på vems vägnar personen undertecknade försäkran samt namnteckning.

BILAGA VI

Förfarande för bedömning av överensstämmelse som grundar sig på intern kontroll

1. Med förfarande för bedömning av överensstämmelse som grundar sig på intern kontroll avses det förfarande för bedömning av överensstämmelse som grundar sig på punkterna 2-4.

2. Leverantören ska kontrollera att det inrättade kvalitetsstyrningssystemet uppfyller kraven i artikel 17.

3. Leverantören ska granska uppgifterna i den tekniska dokumentationen för att bedöma om AI-systemet uppfyller de relevanta grundläggande kraven i kapitel III avsnitt 2.

4. Leverantören ska också kontrollera att utformnings- och utvecklingsprocessen för AI-systemet och övervakningen av detta efter utsläppande på marknaden enligt artikel 72 överensstämmer med den tekniska dokumentationen.

BILAGA VII

Bedömning av överensstämmelse grundad på en bedömning av kvalitetsstyrningssystemet och en bedömning av den tekniska dokumentationen

1. Inledning

Med överensstämmelse som grundar sig på en bedömning av kvalitetsstyrningssystem och en bedömning av den tekniska dokumentationen avses det förfarande för bedömning av överensstämmelse som grundar sig på punkterna 2–5.

2. Översikt

Det godkända kvalitetsstyrningssystemet för utformning, utveckling och testning av AI-system enligt artikel 17 ska granskas i enlighet med punkt 3 och övervakas i enlighet med punkt 5. Den tekniska dokumentationen för AI-systemet ska granskas i enlighet med punkt 4.

3. Kvalitetsstyrningssystem

3.1. Leverantörens ansökan ska innehålla

a) leverantörens namn och adress och, om ansökan lämnas in av ett ombud, även dennes namn och adress,

b) en förteckning över de AI-system som omfattas av samma kvalitetsstyrningssystem,

c) den tekniska dokumentationen för varje AI-system som omfattas av samma kvalitetsstyrningssystem,

d) dokumentationen om kvalitetsstyrningssystemet, som ska omfatta samtliga aspekter som anges i artikel 17,

e) en beskrivning av de förfaranden som har införts för att säkerställa att kvalitetsstyrningssystemet förblir lämpligt och effektivt,

f) en skriftlig försäkran om att samma ansökan inte har lämnats till något annat anmält organ.

3.2. Kvalitetsstyrningssystemet ska bedömas av det anmälda organet, som ska fastställa om det uppfyller kraven i artikel 17.

Beslutet ska meddelas leverantören eller dennes ombud.

Meddelandet ska innehålla slutsatserna från bedömningen av kvalitetsstyrningssystemet och det motiverade bedömningsbeslutet.

3.3. Det godkända kvalitetsstyrningssystemet ska fortsätta att användas och underhållas av leverantören så att det förblir lämpligt och effektivt.

3.4. Leverantören ska underrätta det anmälda organet om alla planerade ändringar av det godkända kvalitetsstyrningssystemet eller förteckningen över de AI-system som omfattas av detta.

De föreslagna ändringarna ska granskas av det anmälda organet, som ska besluta om huruvida det ändrade kvalitetsstyrningssystemet fortfarande uppfyller kraven i punkt 3.2 eller om en ny bedömning är nödvändig.

Det anmälda organet ska meddela leverantören sitt beslut. Meddelandet ska innehålla slutsatserna från granskningen av ändringarna och det motiverade bedömningsbeslutet.

4. Kontroll av den tekniska dokumentationen.

4.1. Utöver den ansökan som avses i punkt 3 ska leverantören lämna in en ansökan till ett valfritt anmält organ för bedömning av den tekniska dokumentationen för det AI-system som leverantören avser att släppa ut på marknaden eller ta i bruk och som omfattas av det kvalitetsstyrningssystem som avses i punkt 3.

4.2. Ansökan ska innehålla

a) leverantörens namn och adress,

b) en skriftlig försäkran om att samma ansökan inte har lämnats in till något annat anmält organ,

c) den tekniska dokumentation som avses i bilaga IV,

4.3. Den tekniska dokumentationen ska granskas av det anmälda organet. ***När så är relevant och begränsat till vad som är nödvändigt för att det anmälda organet ska kunna fullgöra sina uppgifter*** ska det beviljas fullständig åtkomst till de tränings-, ***validerings***- och testdataset som används***, inbegripet, när så är lämpligt och med förbehåll för säkerhetsgarantier,*** genom API eller andra ***relevanta tekniska*** medel och verktyg som möjliggör fjärråtkomst.

4.4. Vid granskningen av den tekniska dokumentationen får det anmälda organet kräva att leverantören lämnar ytterligare bevis eller utför ytterligare tester för att möjliggöra en korrekt bedömning av om AI-systemet uppfyller kraven i kapitel III avsnitt 2. Om det anmälda organet inte nöjer sig med de tester som leverantören har utfört ska det anmälda organet självt direkt utföra lämpliga tester på lämpligt sätt.

4.5. Om det är nödvändigt för att bedöma om AI-systemet med hög risk uppfyller kraven i kapitel III avsnitt 2 ska det anmälda organet, ***efter det att alla andra rimliga sätt att kontrollera överensstämmelse har uttömts och har visat sig vara sig vara otillräckliga,*** och på motiverad begäran också beviljas tillgång till AI-systemets ***träningsmodeller och intränade modeller, inbegripet dess relevanta parametrar. Sådan åtkomst ska omfattas av befintlig unionslagstiftning om skyddet av immateriella rättigheter och företagshemligheter.***

4.6. Det anmälda organets beslut ska meddelas leverantören eller dennes ombud. Anmälan ska innehålla slutsatserna från bedömningen av den tekniska dokumentationen och det motiverade bedömningsbeslutet.

Om AI-systemet uppfyller kraven i kapitel III avsnitt 2 ska ett unionsintyg om bedömning av teknisk dokumentation utfärdas av det anmälda organet. Intyget ska innehålla leverantörens namn och adress, slutsatserna från undersökningen, eventuella giltighetsvillkor och de uppgifter som krävs för att identifiera AI-systemet.

Intyget och dess bilagor ska innehålla alla relevanta uppgifter för att AI-systemets överensstämmelse ska kunna utvärderas och för att AI-systemet ska kunna kontrolleras under användning, i tillämpliga fall.

Om AI-systemet inte uppfyller kraven i kapitel III avsnitt 2 ska det anmälda organet vägra att utfärda ett unionsintyg om bedömning av teknisk dokumentation, underrätta sökanden om detta och utförligt motivera avslaget.

Om AI-systemet inte uppfyller kraven för de data som används för att träna det måste AI-systemet tränas på nytt innan ansökan om en ny bedömning av överensstämmelse lämnas in. I detta fall ska det motiverade bedömningsbeslutet från det anmälda organ som vägrar att utfärda unionsintyget om bedömning av teknisk dokumentation innehålla särskilda överväganden om de kvalitativa data som används för att träna AI-systemet, särskilt om skälen till att kraven inte uppfylls.

4.7. Varje ändring av AI-systemet som kan påverka AI-systemets överensstämmelse med kraven eller dess avsedda ändamål ska bedömas av det anmälda organ som utfärdade unionsintyget om bedömning av teknisk dokumentation. Leverantören ska underrätta det anmälda organet om sin avsikt att utföra någon av de ovannämnda ändringarna eller om den på annat sätt blir medveten om att sådana ändringar har skett. De avsedda ändringarna ska bedömas av det anmälda organet, som ska besluta om dessa ändringar kräver en ny bedömning av överensstämmelse i enlighet med artikel 43.4 eller om de kan åtgärdas genom ett tillägg till unionsintyget om bedömning av teknisk dokumentation. I det senare fallet ska det anmälda organet bedöma ändringarna, underrätta leverantören om sitt beslut och, om ändringarna godkänns, utfärda ett tillägg till unionsintyget om bedömning av teknisk dokumentation, som ska överlämnas till leverantören.

5. Övervakning av det godkända kvalitetsstyrningssystemet.

5.1. Syftet med övervakningen som utförs av det anmälda organ som avses i punkt 3 är att säkerställa att leverantören vederbörligen uppfyller villkoren för det godkända kvalitetsstyrningssystemet.

5.2. För bedömningsändamål ska leverantören ge det anmälda organet tillträde till de lokaler där utformningen, utvecklingen och testningen av AI-systemen äger rum. Leverantören ska vidarebefordra alla nödvändiga uppgifter till det anmälda organet.

5.3. Det anmälda organet ska genomföra periodiskt återkommande revisioner för att försäkra sig om att leverantören upprätthåller och tillämpar kvalitetsstyrningssystemet, samt lämna en revisionsrapport till leverantören. I samband med dessa revisioner får det anmälda organet utföra ytterligare tester av de AI-system för vilka ett unionsintyg om bedömning av teknisk dokumentation har utfärdats.

BILAGA VIII

Uppgifter som ska lämnas in i samband med registreringen
av AI-system med hög risk i enlighet med artikel 49

Avsnitt A – Uppgifter som ska lämnas av leverantörer av AI-system med hög risk i enlighet med artikel 49.1

Följande uppgifter ska lämnas och därefter hållas uppdaterade för de AI-system med hög risk som ska registreras i enlighet med artikel ***49.***1.

1. Leverantörens namn, adress och kontaktuppgifter.
2. Om uppgifterna lämnas av en annan person för leverantörens räkning, dennes namn, adress och kontaktuppgifter.
3. Ombudets namn, adress och kontaktuppgifter, i förekommande fall.
4. AI-systemets handelsnamn och eventuella ytterligare entydiga hänvisningar som gör det möjligt att identifiera och spåra AI-systemet.
5. En beskrivning av AI-systemets avsedda ändamål ***och av de komponenter och funktioner som stöds av detta AI-system.***
6. ***En grundläggande och kortfattad beskrivning av den information som används av systemet (data, indata) och dess operativa logik.***

7. AI-systemets status (på marknaden, eller i bruk; finns inte längre på marknaden/i bruk, har återkallats).

8. Typ, nummer och sista giltighetsdag för det intyg som utfärdats av det anmälda organet samt det anmälda organets namn eller identifikationsnummer, i tillämpliga fall.

9. En skannad kopia av det intyg som avses i punkt 8, i tillämpliga fall.

10. Medlemsstater där AI-systemet har släppts ut på marknaden, tagits i bruk eller tillhandahållits i unionen.

11. En kopia av den EU-försäkran om överensstämmelse som avses i artikel 47.

12. Elektroniska bruksanvisningar. Dessa uppgifter ska inte lämnas för AI-system med hög risk inom områdena brottsbekämpning eller migration, asyl och gränskontrollförvaltning enligt punkterna 1, 6 och 7 i bilaga III.

13. En webbadress för ytterligare information (valfritt).

Avsnitt B – Uppgifter som ska lämnas av leverantörer av AI-system med hög risk i enlighet med artikel 49.2

Följande uppgifter ska lämnas och därefter hållas uppdaterade för de AI-system som ska registreras i enlighet med artikel 49.2.

1. *Leverantörens namn, adress och kontaktuppgifter.*
2. *Om uppgifterna lämnas av en annan person för leverantörens räkning, dennes namn, adress och kontaktuppgifter.*
3. *Ombudets namn, adress och kontaktuppgifter, i förekommande fall.*
4. *AI-systemets handelsnamn och eventuella ytterligare entydiga hänvisningar som gör det möjligt att identifiera och spåra AI-systemet.*
5. *En beskrivning av AI-systemets avsedda ändamål.*
6. *Det eller de villkor enligt artikel 6.3 som ligger till grund för bedömningen att AI-systemet anses vara utan hög risk.*
7. *En kort sammanfattning av de grunder på vilka AI-systemet anses vara utan hög risk vid tillämpning av förfarandet i artikel 6.3.*
8. *AI-systemets status (på marknaden, eller i bruk; finns inte längre på marknaden/i bruk, har återkallats).*
9. *Medlemsstater där AI-systemet har släppts ut på marknaden, tagits i bruk eller tillhandahållits i unionen.*

Avsnitt C – Uppgifter som ska lämnas in av spridare av AI-system med hög risk i enlighet med artikel 49.3

Följande uppgifter ska lämnas och därefter hållas uppdaterade för de AI-system med hög risk som ska registreras i enlighet med artikel 49.

1. ***Spridarens namn, adress och kontaktuppgifter.***
2. ***Namn, adress och kontaktuppgifter för den person som lämnar uppgifter på spridarens vägnar.***
3. ***En sammanfattning av resultaten av den konsekvensbedömning avseende de grundläggande rättigheterna som genomförts i enlighet med artikel 27.***
4. ***Webbadressen för införandet av AI-systemet i EU-databasen av dess leverantör.***
5. ***En sammanfattning av den konsekvensbedömning avseende dataskydd som genomförts i enlighet med artikel 35 i förordning (EU) 2016/679 eller artikel 27 i direktiv (EU) 2016/680, såsom anges i*** artikel 26.8 ***i denna förordning, om så är lämpligt.***

BILAGA IX

Uppgifter som ska lämnas vid registrering av AI-system med hög risk som förtecknas i bilaga III i samband med testning under verkliga förhållanden i enlighet med artikel 60

Följande uppgifter ska lämnas och därefter hållas uppdaterade när det gäller testning under verkliga förhållanden som ska registreras i enlighet med artikel 60:

1. ***Ett enda unionsomfattande identifieringsnumret för testningen under verkliga förhållanden.***
2. ***Namn och kontaktuppgifter för den leverantör eller potentiella leverantör och de spridare som deltar i testningen under verkliga förhållanden.***
3. ***En kort beskrivning av AI-systemet, dess avsedda ändamål och annan information som krävs för att identifiera systemet.***
4. ***En sammanfattning av de viktigaste särdragen i planen för testning under verkliga förhållanden.***
5. ***Information om tillfälligt avbrott eller avslutande av testningen under verkliga förhållanden.***

BILAGA X

Unionslagstiftning om stora it-system på området med frihet, säkerhet och rättvisa

1. Schengens informationssystem

a) Europaparlamentets och rådets förordning (EU) 2018/1860 av den 28 november 2018 om användning av Schengens informationssystem för återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna (EUT L 312, 7.12.2018, s. 1).

b) Europaparlamentets och rådets förordning (EU) 2018/1861 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området in- och utresekontroller, om ändring av konventionen om tillämpning av Schengenavtalet och om ändring och upphävande av förordning (EG) nr 1987/2006 (EUT L 312, 7.12.2018, s. 14).

c) Europaparlamentets och rådets förordning (EU) 2018/1862 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området polissamarbete och straffrättsligt samarbete, om ändring och upphävande av rådets beslut 2007/533/RIF och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1986/2006 och kommissionens beslut 2010/261/EU (EUT L 312, 7.12.2018, s. 56).

2. Informationssystemet för viseringar

a) Europaparlamentets och rådets förordning (EU) 2021/1133 av den 7 juli 2021 om ändring av förordningarna (EU) nr 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 och (EU) 2019/818 vad gäller fastställandet av villkoren för åtkomst till andra EU-informationssystem för ändamål som gäller Informationssystemet för viseringar (EUT L 248, 13.7.2021, s. 1).

b) Europaparlamentets och rådets förordning (EU) 2021/1134 av den 7 juli 2021 om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EG) nr 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 och (EU) 2019/1896 och om upphävande av rådets beslut 2004/512/EG och 2008/633/RIF, i syfte att reformera Informationssystemet för viseringar (EUT L 248, 13.7.2021, s. 11).

3. Eurodac

a) Europaparlamentets och rådets förordning om inrättande av Eurodac för jämförelse av biometriska uppgifter för en effektiv tillämpning av förordning (EU) …/… [förordningen om asyl- och migrationshantering] och förordning (EU) …/… [vidarebosättningsförordningen] och direktiv 2001/55/EG [direktivet om tillfälligt skydd], för identifiering av tredjelandsmedborgare eller statslösa personer som vistas olagligt, och för när medlemsstaternas brottsbekämpande myndigheter och Europol begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordningarna (EU) 2018/1240 och ((EU) 2019/818[+].

[+] EUT: Vänligen för in i texten numret för den förordning som återfinns i dokument PE-CONS 15/24 (2016/0132 (COD)) och för in den förordningens nummer, datum, titel och EUT-hänvisning i fotnoten.

4. In- och utresesystemet

   a) Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017 om inrättande av ett in- och utresesystem för registrering av in- och utreseuppgifter och av uppgifter om nekad inresa för tredjelandsmedborgare som passerar medlemsstaternas yttre gränser, om fastställande av villkoren för åtkomst till in- och utresesystemet för brottsbekämpande ändamål och om ändring av konventionen om tillämpning av Schengenavtalet och förordningarna (EG) nr 767/2008 och (EU) 1077/2011 (EUT L 327, 9.12.2017, s. 20).

5. EU-systemet för reseuppgifter och resetillstånd

   a) Europaparlamentets och rådets förordning (EU) 2018/1240 av den 12 september 2018 om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias) och om ändring av förordningarna (EU) nr 1077/2011, (EU) nr 515/2014, (EU) 2016/399, (EU) 2016/1624 och (EU) 2017/2226 (EUT L 236, 19.9.2018, s. 1).

   b) Europaparlamentets och rådets förordning (EU) 2018/1241 av den 12 september 2018 om ändring av förordning (EU) 2016/794 i syfte att inrätta ett EU-system för reseuppgifter och resetillstånd (Etias) (EUT L 236, 19.9.2018, s. 72).

6. Det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister avseende tredjelandsmedborgare och statslösa personer

   a) Europaparlamentets och rådets förordning (EU) 2019/816 av den 17 april 2019 om inrättande av ett centraliserat system för identifiering av medlemsstater som innehar uppgifter om fällande domar mot tredjelandsmedborgare och statslösa personer (Ecris-TCN) för att komplettera det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister och om ändring av förordning (EU) 2018/1726 (EUT L 135, 22.5.2019, s. 1).

7. Interoperabilitet

   a) Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar (EUT L 135, 22.5.2019, s. 27).

   b) Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och migration (EUT L 135, 22.5.2019, s. 85).

BILAGA XI

Teknisk dokumentation som avses i artikel 53.1 a – teknisk dokumentation för leverantörer av AI-modeller för allmänna ändamål

Avsnitt 1

Information som ska tillhandahållas av samtliga leverantörer av AI-modeller för allmänna ändamål

Den tekniska dokumentation som avses i artikel 53.1 a ***ska minst innehålla följande information, beroende på vad som är lämpligt med avseende på modellens storlek och riskprofil:***

1. En allmän beskrivning av AI-systemet för allmänna ändamål, inklusive

a) de uppgifter som modellen är avsedd att utföra och typen och arten av AI-system i vilka den kan integreras,

b) tillämpliga riktlinjer för godtagbar användning,

c) datum för frisläppande och distributionsmetoder,

d) parametrarnas struktur och antal,

e) metod (t.ex. text, bild) och format för in- och utdata,

f) licensen.

2. En utförlig beskrivning av delarna i den modell som avses i punkt 1 och relevant information om utvecklingsprocessen, inbegripet följande:

a) De tekniska medel (t.ex. bruksanvisningar, infrastruktur, verktyg) som krävs för att AI-modellen för allmänna ändamål ska integreras i AI-system.

b) Modellens och träningsprocessens designspecifikationer, inbegripet metoder och teknik för träningen, de viktigaste designvalen, inklusive motiveringen och de antaganden som gjorts, vad modellen har utformats för att optimera och de olika parametrarnas relevans, i förekommande fall.

c) Information om de data som används för träning, testning och validering, i tillämpliga fall, inbegripet datatyp och härkomst för data och kurateringsmetoder (t.ex. rensning, filtrering osv.), antal datapunkter, deras omfattning och huvudsakliga egenskaper, hur data inhämtades och valdes ut samt alla andra åtgärder för att upptäcka datakällor och metoder för att upptäcka identifierbara snedvridningar, i tillämpliga fall.

d) De dataresurser som används för att träna modellen (t.ex. antal flyttalsberäkningar), träningstid och andra relevanta uppgifter som rör träningen.

e) Känd eller uppskattad energiförbrukning för modellen.

När det gäller led e, om modellens energiförbrukning är okänd, får uppgiften om energiförbrukningen baseras på information om de dataresurser som används.

Avsnitt 2

Ytterligare information som ska tillhandahållas av samtliga leverantörer av AI-modeller för allmänna ändamål

1. En utförlig beskrivning av utvärderingsstrategierna, inklusive utvärderingsresultaten, på grundval av tillgängliga offentliga utvärderingsprotokoll och utvärderingsverktyg eller annars av andra utvärderingsmetoder. Utvärderingsstrategierna ska omfatta utvärderingskriterier, mått och metoder för identifiering av begränsningar.

2. I tillämpliga fall, en utförlig beskrivning av de åtgärder som vidtagits för att genomföra intern och/eller extern antagonistisk testning (t.ex. red teaming), modellanpassningar, inklusive harmonisering och finjustering.

3. I tillämpliga fall en utförlig beskrivning av systemarkitekturen som förklarar hur programvarukomponenter bygger på eller påverkar varandra och integreras i den övergripande behandlingen.

BILAGA XII

Transparensinformation som avses i artikel 53.1 b

– teknisk dokumentation för leverantörer av AI-modeller för allmänna ändamål till leverantörer i efterföljande led som integrerar modellen i sina AI-system

Den information som avses i artikel 53.1 b ska minst innehålla följande:

1. En allmän beskrivning av AI-systemet för allmänna ändamål, inklusive

a) de uppgifter som modellen är avsedd att utföra och typen och arten av AI-system i vilka den kan integreras,

b) tillämpliga riktlinjer för godtagbar användning,

c) datum för frisläppande och distributionsmetoder,

d) hur modellen interagerar eller kan användas för att interagera med maskinvara eller programvara som inte ingår i själva modellen, i tillämpliga fall,

e) versionerna av relevant programvara som rör användningen av AI-modellen för allmänna ändamål, i tillämpliga fall,

f) parametrarnas struktur och antal,

g) metod (t.ex. text, bild) och format för in- och utdata,

h) licensen för modellen.

2. En beskrivning av modellens komponenter och dess utvecklingsprocess, inklusive

a) de tekniska medel (t.ex. bruksanvisningar, infrastruktur, verktyg) som krävs för att AI-modellen för allmänna ändamål ska integreras i AI-system,

b) metod (t.ex. text, bild osv.) och format för in- och utdata och deras maximala storlek (t.ex. kontextfönstrets längd osv.),

c) information om de data som används för träning, testning och validering, i tillämpliga fall, inbegripet datatyp, varifrån dessa data kommer och kurateringsmetoder.

BILAGA XIII

Kriterier för utseende av AI-modeller för allmänna ändamål med systemrisk som avses i artikel 51

Vid fastställandet av att en AI-modell för allmänna ändamål har kapacitet eller effekter som motsvarar dem som anges i artikel 51.1 a och b ska kommissionen beakta följande kriterier:

a) ***Antalet parametrar i modellen.***

b) ***Datasetets kvalitet eller storlek, till exempel mätt genom token.***

c) ***Den beräkningsmängd som används för att träna modellen, mätt i flyttalsberäkningar eller angiven med en kombination av andra variabler, såsom beräknad träningskostnad, uppskattad tid som krävs för träningen eller uppskattad energiförbrukning för träningen.***

d) ***Modellens in- och utmatningsmetoder, såsom text till text (stora språkmodeller), text till bild, multimodalitet och aktuella tröskelvärden för att fastställa kapacitet med hög påverkansgrad för varje metod, och den specifika typen av in- och utdata (t.ex. biologiska sekvenser).***

e) ***Riktmärken för och utvärderingar av modellens kapacitet, inbegripet med beaktande av antalet uppgifter utan ytterligare träning, anpassningsförmåga att lära sig nya, distinkta uppgifter, dess grad av autonomi och skalbarhet samt de verktyg som den har tillgång till.***

f) ***Huruvida modellen har stor inverkan på den inre marknaden på grund av sin räckvidd, vilket ska förutsättas om den har gjorts tillgänglig för minst 10 000 registrerade företagsanvändare som är etablerade i unionen.***

g) ***Antalet registrerade slutanvändare.***

Departementsserien 2024

Kronologisk förteckning

1. Ändrade regler om tillsyn m.m. över Totalförsvarets forskningsinstitut. Fö.
2. Avtal om försvarssamarbete med Amerikas förenta stater. Fö.
3. Partipolitiska lotterier. Fi.
4. Ett digitalt utvecklingsstöd till vissa tidskrifter. Ku.
5. Sociala grundvillkor i den gemensamma jordbrukspolitiken. LI.
6. Stärkt försvarsförmåga. Sverige som allierad. Fö.
7. Avskildhet vid dygnsvilan. En delredovisning angående frågor om Statens institutionsstyrelses särskilda befogenheter. S.
8. Förbättrat informationsutbyte mellan Arbetsförmedlingen och kommuner. A.
9. Bättre förutsättningar för utsänd statlig personal. UD.
10. Stärkt skydd för vissa förtroendevalda och en tydligare intern kontroll i kommuner och regioner. Fi.
11. Förbättrade möjligheter för polisen att använda kamerabevakning. Ju.

Departementsserien 2024

Systematisk förteckning

Arbetsmarknadsdepartementet

Förbättrat informationsutbyte mellan Arbetsförmedlingen och kommuner. [8]

Finansdepartementet

Partipolitiska lotterier. [3]

Stärkt skydd för vissa förtroendevalda och en tydligare intern kontroll i kommuner och regioner. [10]

Försvarsdepartementet

Ändrade regler om tillsyn m.m. över Totalförsvarets forskningsinstitut. [1]

Avtal om försvarssamarbete med Amerikas förenta stater. [2]

Stärkt försvarsförmåga. Sverige som allierad. [6]

Justitiedepartementet

Förbättrade möjligheter för polisen att använda kamerabevakning. [11]

Kulturdepartementet

Ett digitalt utvecklingsstöd till vissa tidskrifter. [4]

Landsbygds- och infrastrukturdepartementet

Sociala grundvillkor i den gemensamma jordbrukspolitiken. [5]

Socialdepartementet

Avskildhet vid dygnsvilan. En delredovisning angående frågor om Statens institutionsstyrelses särskilda befogenheter. [7]

Utrikesdepartementet

Bättre förutsättningar för utsänd statlig personal. [9]