Europeiska unionens råd

Bryssel den 25 november 2022
(OR. en)

14954/22

Interinstitutionellt ärende:
2021/0106(COD)

LIMITE

TELECOM 472
JAI 1494
COPEN 396
CYBER 374
DATAPROTECT 320
EJUSTICE 89
COSI 293
IXIM 267
ENFOPOL 569
RELEX 1556
MI 843
COMPET 918
CODEC 1773

NOT

från:	Ständiga representanternas kommitté (Coreper I)
till:	Rådet
Föreg. dok. nr:	14336/22
Komm. dok. nr:	8115/21
Ärende:	Förslag till Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter – Allmän riktlinje

I. INLEDNING

1. Den 21 april 2021 antog kommissionen förslaget till förordning om harmoniserade regler för artificiell intelligens **(rättsakt om artificiell intelligens)**.

2. Målen för kommissionens förslag är att säkerställa att AI-system som släpps ut på unionsmarknaden och används i unionen är säkra och är förenliga med befintlig lagstiftning om grundläggande rättigheter och unionens värden, att säkerställa rättssäkerhet för att underlätta investeringar och innovation för AI, att förbättra styrningen och den faktiska efterlevnaden av befintlig lagstiftning om de grundläggande rättigheterna och säkerhet samt att främja utvecklingen av en inre marknad för lagliga, säkra och tillförlitliga AI-tillämpningar, samtidigt som man förhindrar marknadsfragmentering.

II. ARBETET I DE ÖVRIGA INSTITUTIONERNA

3. I Europaparlamentet leds diskussionerna av utskottet för den inre marknaden och konsumentskydd (IMCO, med Brando Benifei, S&D, Italien, som föredragande) och utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor (LIBE, med Dragos Tudorache, Renew, Rumänien, som föredragande) inom ramen för ett förfarande med gemensamma utskottssammanträden. Utskottet för rättsliga frågor (JURI), utskottet för industrifrågor, forskning och energi (ITRE) och utskottet för kultur och utbildning (CULT) är associerade till lagstiftningsarbetet med delade och/eller exklusiva befogenheter. De två medföredragandena presenterade sitt förslag till betänkande i april 2022, och omröstningen om det gemensamma IMCO-LIBE-betänkandet planeras till första kvartalet 2023.

4. Europeiska ekonomiska och sociala kommittén avgav sitt yttrande om förslaget den 22 september 2021, medan Europeiska regionkommittén följde efter med sitt yttrande den 2 december 2021.

5. Den 18 juni 2021 avgav Europeiska dataskyddsstyrelsen (EDPB) och Europeiska datatillsynsmannen (EDPS) ett gemensamt yttrande om förslaget.

6. ECB avgav sitt yttrande den 29 december 2021 och lade fram det inför arbetsgruppen för telekommunikation och informationssamhället (*arbetsgruppen för telekommunikation*) den 10 februari 2022.

III. LÄGESRAPPORT OM RÅDETS ARBETE

1. I rådet behandlades förslaget i arbetsgruppen för telekommunikation. Arbetsgruppen för telekommunikation började behandla förslaget under det portugisiska ordförandeskapet vid flera möten och workshoppar som hölls mellan april och juni 2021. Arbetet med förslaget fortsatte under det slovenska ordförandeskapet, som utarbetade det första partiella kompromissförslaget som omfattade **artiklarna 1–7 och bilagorna I–III**. Dessutom anordnade det slovenska ordförandeskapet ett informellt halvdagsmöte i rådet med telekommunikationsministrarna där man uteslutande ägnade sig åt förslaget till rättsakt om artificiell intelligens. Ministrarna bekräftade då sitt stöd för den övergripande och människocentrerade strategin för att reglera AI. Det franska ordförandeskapet fortsatte granskningsprocessen och ändrade i slutet av sin mandatperiod de återstående delarna av texten **(artiklarna 8–85 och bilagorna IV–IX)** och lade fram hela det första konsoliderade kompromissförslaget om AI-rättsakten den 17 juni 2022.

2. Den 5 juli 2022 höll det tjeckiska ordförandeskapet en riktlinjedebatt i arbetsgruppen för telekommunikation på grundval av ett dokument om politiska alternativ, vars resultat användes för att utarbeta **det andra kompromissförslaget**. På grundval av delegationernas reaktioner på denna kompromiss utarbetade det tjeckiska ordförandeskapet **det tredje kompromissförslaget**, som lades fram och diskuterades i arbetsgruppen för telekommunikation den 22 och 29 september 2022. Efter dessa diskussioner ombads delegationerna att lämna ytterligare skriftliga kommentarer, som det tjeckiska ordförandeskapet använde för att utarbeta **det fjärde kompromissförslaget**. På grundval av diskussionerna om det fjärde kompromissförslaget i arbetsgruppen för telekommunikation den 25 oktober 2022 och den 8 november 2022 och med beaktande av medlemsstaternas slutliga skriftliga kommentarer har det tjeckiska ordförandeskapet utarbetat **den slutliga versionen av kompromissförslaget**, som återfinns i bilagan. Den 18 november behandlade Coreper detta kompromissförslag och **enades enhälligt om att lägga fram det för rådet (transport, telekommunikation och energi) utan ändringar inför en allmän riktlinje** vid mötet den 6 december 2022.

IV. KOMPROMISSFÖRSLAGETS VIKTIGASTE INSLAG

1. Definition av AI-system, förbjudna AI-tillämpningar, förteckning över fall av användning av AI med hög risk i bilaga III och klassificering av AI-system som högrisksystem

1.1 För att säkerställa att definitionen av AI-system innehåller tillräckligt tydliga kriterier för att skilja AI från mer klassiska programvarusystem begränsas definitionen i **artikel 3.1** i kompromissförslaget till system som utvecklats genom metoder för maskininlärning och logik- och kunskapsbaserade metoder.

1.2 När det gäller delegeringen av befogenheter till kommissionen i samband med uppdateringarna av definitionen av AI-system har **bilaga I** och motsvarande befogenhet för kommissionen att uppdatera den genom delegerade akter utgått. I stället har nya skäl **6a och 6b** lagts till för att klargöra vad som avses med metoder för maskininlärning och logik- och kunskapsbaserade metoder. För att säkerställa att AI-rättsakten förblir flexibel och framtidssäkrad har en möjlighet att anta genomförandeakter för att ytterligare specificera och uppdatera teknik inom ramen för maskininlärningsmetoder och logik- och kunskapsbaserade strategier lagts till i **artikel 4**.

1.3 När det gäller förbjudna AI-tillämpningar innehåller kompromissförslaget i **artikel 5** en utvidgning av förbudet mot att använda AI för social poängsättning till att även omfatta privata aktörer. Dessutom omfattar bestämmelsen om förbud mot användning av AI-system som utnyttjar sårbarheter hos en specifik grupp av personer nu även personer som är sårbara på grund av sin sociala eller ekonomiska situation. När det gäller förbudet för brottsbekämpande myndigheter att använda system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser klargörs i kompromissförslaget de mål där sådan användning anses vara absolut nödvändig för brottsbekämpande ändamål och för vilka de brottsbekämpande myndigheterna därför undantagsvis bör tillåtas att använda sådana system.

1.4 När det gäller förteckningen över fall av användning av AI med hög risk i **bilaga III** har tre av dem strukits (brottsbekämpande myndigheters upptäckt av deepfakes, brottsanalys och kontroll av resehandlingars äkthet), medan två har lagts till (kritisk digital infrastruktur och liv- och sjukförsäkring) och andra har finjusterats. Samtidigt har **artikel 7.1** ändrats för att göra det möjligt att inte bara lägga till fall av användning med hög risk i förteckningen genom delegerade akter, utan även att stryka dem. För att säkerställa att de grundläggande rättigheterna skyddas på lämpligt sätt vid sådana strykningar har ytterligare bestämmelser lagts till i **artikel 7.3** som specificerar de villkor som måste uppfyllas innan en delegerad akt kan antas.

1.5 När det gäller klassificeringen av AI-system som högrisksystem innehåller kompromissförslaget nu ett ytterligare horisontellt skikt, utöver den klassificering av hög risk som görs i **bilaga III**, för att säkerställa att AI-system som sannolikt inte orsakar allvarliga kränkningar av de grundläggande rättigheterna eller andra betydande risker inte omfattas. Mer specifikt innehåller **artikel 6.3** nya bestämmelser enligt vilka betydelsen av AI-systemets utdata med avseende på den relevanta åtgärden eller ett beslut som ska fattas också bör beaktas när AI-system klassificeras som högrisksystem. Betydelsen av ett AI-systems utdata skulle bedömas på grundval av huruvida de är rent accessoriska med avseende på den relevanta åtgärd som ska vidtas eller det relevanta beslut som ska fattas.

2. Krav på AI-system med hög risk och ansvaret för olika aktörer i AI-värdekedjan

2.1 Många av kraven för AI-system med hög risk och som föreskrivs i **avdelning III kapitel 2** i förslaget, har förtydligats och justerats på ett sådant sätt att de är mer tekniskt genomförbara och mindre betungande för berörda parter att uppfylla, till exempel när det gäller kvaliteten på data, eller i förhållande till den tekniska dokumentation som bör utarbetas av små och medelstora företag för att visa att deras AI-system med hög risk uppfyller kraven.

2.2 Med tanke på att AI-system utvecklas och distribueras genom komplexa värdekedjor innehåller kompromissförslaget ändringar som klargör ansvars- och rollfördelningen. Till exempel har några bestämmelser i **artiklarna 13 och 14** lagts till för att möjliggöra ett effektivare samarbete mellan leverantörer och användare. Kompromisstexten syftar också till att klargöra förhållandet mellan ansvarsområdena enligt AI-rättsakten och de ansvarsområden som redan finns enligt annan lagstiftning, såsom relevant unionslagstiftning om dataskydd eller sektorsspecifik lagstiftning, inbegripet när det gäller sektorn för finansiella tjänster. I den nya **artikel 23a** anges dessutom tydligare i vilka situationer andra aktörer i värdekedjan är skyldiga att ta på sig en leverantörs ansvar.

3. AI-system för allmänna ändamål

3.1 En ny **avdelning IA** har lagts till för att ta hänsyn till situationer där AI-system kan användas för många olika ändamål (AI för allmänna ändamål) och där det kan finnas omständigheter där AI-teknik för allmänna ändamål integreras i ett annat system som kan bli ett högrisksystem. I kompromissförslaget anges i **artikel 4b.1** att vissa krav för AI-system med hög risk också ska tillämpas på AI-system för allmänna ändamål. I stället för direkt tillämpning av dessa krav skulle dock en genomförandeakt specificera hur de bör tillämpas i förhållande till AI-system för allmänna ändamål, på grundval av ett samråd och en närmare konsekvensbedömning samt med beaktande av dessa systems särdrag och tillhörande värdekedja, teknisk genomförbarhet samt marknadsutveckling och teknisk utveckling. Genom att en genomförandeakt används säkerställs att medlemsstaterna involveras ordentligt och har sista ordet när det gäller hur kraven kommer att tillämpas i detta sammanhang.

3.2 Kompromisstexten i **artikel 4b.5** innehåller också en möjlighet att anta ytterligare genomförandeakter som fastställer formerna för samarbete mellan leverantörer av AI-system för allmänna ändamål och andra leverantörer som avser att ta sådana system i bruk eller släppa ut sådana system på unionsmarknaden som AI-system med hög risk, särskilt när det gäller tillhandahållande av information.

4. **Förtydligande av tillämpningsområdet för den föreslagna AI-rättsakten och bestämmelser om brottsbekämpande myndigheter**

4.1 I **artikel 2** har en uttrycklig hänvisning gjorts till att ändamål som rör nationell säkerhet och försvar samt militära ändamål inte omfattas av AI-rättsaktens tillämpningsområde. På samma sätt har det klargjorts att AI-rättsakten inte bör tillämpas på AI-system och deras utdata om de enbart används för forskning och utveckling och på skyldigheter för personer som använder AI för icke-yrkesmässiga ändamål, vilket skulle falla utanför AI-rättsaktens tillämpningsområde, med undantag för transparenskraven.

4.2 För att ta hänsyn till det som specifikt kännetecknar brottsbekämpande organ har ett antal ändringar av bestämmelserna om användning av AI-system för brottsbekämpande ändamål gjorts. Framför allt har vissa av de relaterade definitionerna i **artikel 3**, såsom *system för biometrisk fjärridentifiering* och *system för biometrisk fjärridentifiering i realtid*, finjusterats för att klargöra vilka situationer som skulle omfattas av det relaterade förbudet och högriskfallet av användning och vilka situationer som inte skulle göra det. Kompromissförslaget innehåller också andra ändringar som, med förbehåll för lämpliga skyddsåtgärder, är avsedda att säkerställa en lämplig grad av flexibilitet vid brottsbekämpande myndigheters användning av AI-system med hög risk eller avspegla behovet av att respektera konfidentialiteten för känsliga operativa uppgifter i samband med dessa myndigheters verksamhet.

5. **Bedömningar av överensstämmelse, styrningsram, marknadskontroll, efterlevnad och påföljder**

5.1 För att förenkla regelverket för efterlevnad av AI-rättsakten innehåller kompromissförslaget ett antal förtydliganden och förenklingar av bestämmelserna om förfaranden för bedömning av överensstämmelse. Bestämmelserna om marknadskontroll har också förtydligats och förenklats för att göra dem mer effektiva och lättare att genomföra, med beaktande av behovet av ett proportionellt tillvägagångssätt i detta avseende. Dessutom har **artikel 41** setts över grundligt för att begränsa kommissionens utrymme för skönsmässig bedömning när det gäller antagandet av genomförandeakter om fastställande av gemensamma tekniska specifikationer för kraven för AI-system med hög risk och AI-system för allmänna ändamål.

5.2 Genom kompromissförslaget har också bestämmelserna för nämnden för artificiell intelligens (*nämnden*) ändrats väsentligt i syfte att säkerställa större autonomi och stärka dess roll i styrningsstrukturen för AI-rättsakten. I detta sammanhang har **artiklarna 56 och 58** reviderats för att stärka nämndens roll på ett sådant sätt att den bör ha bättre förutsättningar att ge stöd till medlemsstaterna i genomförandet och efterlevnaden av AI-rättsakten. Mer specifikt har nämndens uppgifter utökats och dess sammansättning har specificerats. För att säkerställa de berörda parternas deltagande i alla frågor som rör genomförandet av AI-rättsakten, inbegripet utarbetandet av genomförandeakter och delegerade akter, har ett nytt krav lagts till på att nämnden ska inrätta en ständig arbetsgrupp som fungerar som en plattform för ett brett spektrum av berörda parter. Två andra ständiga arbetsgrupper för marknadskontrollmyndigheter och anmälande myndigheter bör också inrättas för att stärka enhetligheten i styrningen och efterlevnaden av AI-rättsakten i hela unionen.

5.3 För att ytterligare förbättra styrningsramen innehåller kompromisstexten de nya artiklarna **68a och 68b**. **Artikel 68a** innehåller kravet att kommissionen ska utse en eller flera unionstestanläggningar på området artificiell intelligens, som bör tillhandahålla oberoende teknisk eller vetenskaplig rådgivning på begäran av nämnden eller marknadskontrollmyndigheterna, medan **artikel 68b** skapar en skyldighet för kommissionen att inrätta en central pool av oberoende experter för att stödja den tillsynsverksamhet som krävs enligt AI-rättsakten. Slutligen finns det också en ny artikel **58a** som fastställer en skyldighet för kommissionen att ta fram riktlinjer för tillämpningen av AI-rättsakten.

5.4 När det gäller påföljderna för överträdelser av bestämmelserna i AI-rättsakten föreskrivs i **artikel 71** i kompromissförslaget mer proportionella tak för administrativa sanktionsavgifter för små och medelstora företag och nystartade företag. Dessutom har ytterligare fyra kriterier lagts till i **artikel 71.6** för fastställande av storleken på administrativa sanktionsavgifter för att ytterligare säkerställa deras övergripande proportionalitet.

6. Transparensbestämmelser och andra bestämmelser till förmån för de berörda personerna

6.1 Kompromissförslaget innehåller ett antal ändringar som ökar transparensen när det gäller användningen av AI-system med hög risk. Framför allt har **artikel 51** uppdaterats för att ange att vissa användare av AI-system med hög risk som är offentliga myndigheter, byråer eller organ också kommer att vara skyldiga att registrera sig i den unionsdatabas för AI-system med hög risk som förtecknas i bilaga III. I den nyligen tillagda artikel **52.2a** betonas dessutom en skyldighet för användare av ett system för känsloigenkänning att informera fysiska personer när de utsätts för ett sådant system.

6.2 Kompromissförslaget klargör också i den nytillagda artikel **63.11** att en fysisk eller juridisk person som har skäl att anse att bestämmelserna i AI-rättsakten har överträtts får lämna in ett klagomål till den berörda marknadskontrollmyndigheten och förvänta sig att ett sådant klagomål kommer att behandlas i enlighet med den myndighetens särskilda förfaranden.

7. Åtgärder till stöd för innovation

7.1 I syfte att skapa en rättslig ram som är mer innovationsvänlig och för att främja evidensbaserat regulatoriskt lärande har bestämmelserna om åtgärder till stöd för innovation i **artikel 53** ändrats väsentligt i kompromissförslaget. För det första har det klargjorts att regulatoriska sandlådor för AI, som förväntas skapa en kontrollerad miljö för utveckling, testning och validering av innovativa AI-system under de nationella behöriga myndigheternas direkta tillsyn och vägledning, också bör göra det möjligt att testa innovativa AI-system under verkliga förhållanden. Dessutom har nya bestämmelser i **artiklarna 54a och 54b** lagts till för att möjliggöra oövervakad testning av AI-system under verkliga förhållanden enligt särskilda villkor och skyddsåtgärder. I båda fallen klargörs i kompromissförslaget hur dessa nya regler ska tolkas i förhållande till annan befintlig sektorslagstiftning om regulatoriska sandlådor.

7.2 För att minska den administrativa bördan för mindre företag innehåller kompromissförslaget i **artikel 55** en förteckning över åtgärder som kommissionen ska vidta för att stödja sådana operatörer, och i **artikel 55a** föreskrivs vissa begränsade och tydligt specificerade undantag.

V. SLUTSATS

1. Mot bakgrund av ovanstående uppmanas rådet att
   - behandla det bifogade kompromissförslaget,
   - bekräfta en allmän riktlinje om förslaget till förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) vid mötet i rådet (transport, telekommunikation och energi) den 6 december 2022.

_____

BILAGA

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

OM HARMONISERADE REGLER FÖR ARTIFICIELL INTELLIGENS (RÄTTSAKT OM ARTIFICIELL INTELLIGENS) OCH OM ÄNDRING AV VISSA UNIONSLAGSTIFTNINGSAKTER

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT [DENNA FÖRORDNING/DETTA DIREKTIV/DETTA BESLUT]

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 Regionkommitténs yttrande[2],

med beaktande av Europeiska centralbankens yttrande[3],

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

---

1 EUT C […], […], s. […].
2 EUT C […], […], s. […].
3 Hänvisning till ECB:s yttrande.

(1) Syftet med denna förordning är att förbättra den inre marknadens funktionssätt genom att fastställa en enhetlig rättslig ram för i synnerhet utveckling, saluföring och användning av artificiell intelligens i enlighet med unionens värden. Denna förordnings syften baseras på ett antal tvingande hänsyn till allmänintresset, såsom en hög skyddsnivå för hälsa, säkerhet och grundläggande rättigheter, och säkerställer fri rörlighet över gränserna för AI-baserade varor och tjänster, vilket förhindrar att medlemsstaterna inför begränsningar av utvecklingen, saluföringen och användningen av AI-system, om sådana inte uttryckligen tillåts enligt denna förordning.

(2) System med artificiell intelligens (AI-system) kan enkelt användas inom många olika ekonomiska sektorer och samhällssektorer, inklusive över gränser, och cirkulera i hela unionen. Vissa medlemsstater har redan undersökt antagandet av nationella regler för att säkerställa att artificiell intelligens är säker och att den utvecklas och används i enlighet med skyldigheter som rör grundläggande rättigheter. Olikartade 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, och avvikelser som hindrar den fria rörligheten för 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, baserat på artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget). I den utsträckning som förordningen omfattar särskilda regler för skydd av individer när det gäller behandling av personuppgifter i samband med användning av AI-system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser i brottsbekämpande syfte, är det, när det gäller dessa särskilda regler, lämpligt att basera 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.

(3) Artificiell intelligens tillhör en teknikfamilj under snabb utveckling som kan bidra till en mängd ekonomiska och samhälleliga vinster över hela spektrumet av näringslivssektorer och samhällsverksamheter. Artificiell intelligens kan ge bättre prognoser, optimera verksamheter och resurstilldelning och individanpassa digitala lösningar som finns tillgängliga för enskilda och organisationer och på så sätt ge företagen viktiga konkurrensfördelar och stödja socialt och miljömässigt fördelaktiga utfall, exempelvis inom hälso- och sjukvård, jordbruk, utbildning, infrastrukturförvaltning, energi, transport och logistik, offentliga tjänster, säkerhet, rättsväsen, resurs- och energieffektivitet samt begränsning av och anpassning till klimatförändringar.

(4) Samtidigt kan artificiell intelligens, beroende på omständigheterna kring den specifika tillämpningen och användningen, ge upphov till risker och skada allmänna intressen och rättigheter som skyddas av unionsrätten. Dessa skador kan vara materiella eller immateriella.

(5) Därmed behövs en rättslig ram för unionen som omfattar harmoniserade regler för artificiell intelligens, för att främja utvecklingen, användningen och spridningen av artificiell intelligens på den inre marknaden, och som samtidigt uppnår en hög skyddsnivå för allmänintressen, såsom hälsa, säkerhet och skydd av grundläggande rättigheter, som erkänns och är skyddade enligt unionsrätten. För att uppnå detta syfte bör det fastställas regler som reglerar utsläppandet på marknaden och ibruktagandet 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. Genom fastställandet av dessa regler och på grundval av arbetet i högnivåexpertgruppen för artificiell intelligens, såsom detta avspeglas i riktlinjerna för tillförlitlig artificiell intelligens, stöder denna förordning unionens mål att bli världsledande inom utvecklingen av säker, tillförlitlig och etisk artificiell intelligens, såsom fastställts av Europeiska rådet[4], och säkerställer skyddet av etiska principer, vilket särskilt har begärts av Europaparlamentet[5].

---

[4] Europeiska rådet, extra möte i Europeiska rådet (den 1 och 2 oktober 2020) – Slutsatser, EUCO 13/20, 2020, s. 6.

[5] 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)).

(5a) De harmoniserade regler om utsläppande på marknaden, ibruktagande och användning av AI-system som fastställs i denna förordning bör gälla i alla sektorer och bör, i linje med dess strategi för en ny lagstiftningsram, inte påverka befintlig unionslagstiftning, särskilt om dataskydd, konsumentskydd, grundläggande rättigheter, sysselsättning och produktsäkerhet, vilken denna förordning kompletterar. Som en följd av detta påverkas inte några rättigheter eller rättsmedel som unionsrätten ger konsumenter och andra personer som kan påverkas negativt av AI-system, inbegripet vad gäller ersättning för eventuella skador i enlighet med rådets direktiv 85/374/EEG av den 25 juli 1985 om tillnärmning av medlemsstaternas lagar och andra författningar om skadeståndsansvar för produkter med säkerhetsbrister, och de förblir fullt tillämpliga. 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 tillämpningen av nationell lagstiftning, i överensstämmelse 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 mån de inte är specifika för AI-system och eftersträvar andra legitima mål av allmänt intresse, inte påverkas av denna förordning.

(6) Begreppet AI-system bör vara tydligt definierat för att säkerställa rättssäkerhet och samtidigt ge den flexibilitet som behövs för anpassning till framtida teknisk utveckling. Definitionen bör baseras på viktiga funktionella egenskaper hos artificiell intelligens, såsom dess inlärnings-, resonemangs- eller modelleringskapacitet, och skilja den från enklare programvarusystem och programmeringsmetoder. I synnerhet bör AI-system, vid tillämpningen av denna förordning, på grundval av maskin- och/eller människobaserade data och indata, kunna dra slutsatser om hur man kan uppnå en uppsättning slutliga mål som människor har gett dem, med hjälp av maskininlärning och/eller logik- och kunskapsbaserade metoder, och producera resultat såsom innehåll för generativa AI-system (t.ex. text, video eller bilder), förutsägelser, rekommendationer eller beslut, som påverkar den miljö med vilken systemet interagerar, i en fysisk eller digital dimension. Ett system som använder regler som enbart definieras av fysiska personer för att automatiskt utföra operationer bör inte anses vara ett AI-system. AI-system kan utformas för att arbeta med olika nivåer av autonomi och 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). Begreppet ett AI-systems autonomi avser den utsträckning i vilken ett sådant system fungerar utan mänsklig medverkan.

(6a) Metoder för maskininlärning är inriktade på att utveckla system som kan lära sig och dra slutsatser av data för att lösa ett tillämpningsproblem utan att uttryckligen programmeras med en uppsättning steg-för-steg-instruktioner från inmatning till utdata. Inlärning avser beräkningsprocessen för att utifrån data optimera parametrarna för modellen, som är en matematisk konstruktion som genererar utdata baserat på indata. De olika problem som kan lösas genom maskininlärning omfattar vanligtvis uppgifter för vilka andra metoder misslyckas, antingen på grund av att det inte finns någon lämplig formalisering av problemet eller på grund av att det är svårt att lösa problemet med icke-inlärningsmetoder. Maskininlärningsmetoder omfattar till exempel övervakat, oövervakat och förstärkt lärande, med användning av en rad olika metoder, bland annat djupinlärning med neurala nätverk, statistiska metoder för inlärning och inferens (t.ex. logistisk regression, Bayesiansk beräkning) samt sök- och optimeringsmetoder.

(6b) Logik- och kunskapsbaserade metoder är inriktade på utveckling av system med logisk resonemangskapacitet för kunskap för att lösa ett tillämpningsproblem. Sådana system omfattar vanligtvis en kunskapsbas och en inferensmaskin som genererar resultat genom att resonera om kunskapsbasen. Kunskapsbasen, som vanligtvis kodas av mänskliga experter, representerar enheter och logiska relationer som är relevanta för tillämpningsproblemet genom formaliseringar baserade på regler, ontologier eller kunskapsdiagram. Inferensmaskinen påverkar kunskapsbasen och extraherar ny information genom t.ex. sortering, sökning, matchning eller chaining. Logik- och kunskapsbaserade metoder omfattar t.ex. kunskapsrepresentation, induktiv (logisk) programmering, kunskapsbaser, inferens- och deduktionsmaskiner, (symboliska) resonemang, expertsystem samt sök- och optimeringsmetoder.

(6c) för att säkerställa enhetliga villkor för genomförandet av denna förordning när det gäller metoder för maskininlärning och logik- och kunskapsbaserade metoder, och för att ta hänsyn till marknadsutvecklingen och den tekniska utvecklingen, bör kommissionen tilldelas genomförandebefogenheter.

(6d) Begreppet *användare* som avses i denna förordning bör tolkas som varje fysisk eller juridisk person, inbegripet en offentlig myndighet, en byrå eller ett annat organ, som använder ett AI-system och under vars överinseende systemet används. Beroende på typen av AI-system kan användningen av systemet påverka andra personer än användaren.

(7) Begreppet biometriska uppgifter, som används i denna förordning bör tolkas i överensstämmelse med begreppet biometriska uppgifter enligt definitionen i artikel 4.14 i Europaparlamentets och rådets förordning (EU) 2016/679[6], artikel 3.18 i Europaparlamentets och rådets förordning (EU) 2018/1725[7] och artikel 3.13 i Europaparlamentets och rådets direktiv (EU) 2016/680[8].

[6] 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).

[7] 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).

[8] 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 (direktivet om brottsbekämpning) (EUT L 119, 4.5.2016, s. 89).

(8) Begreppet system för biometrisk fjärridentifiering enligt denna förordning bör definieras utifrån funktion, som ett AI-system avsett för identifiering av fysiska personer, vanligtvis på distans, utan deras aktiva medverkan, genom jämförelse mellan en persons biometriska uppgifter och biometriska uppgifter i ett referenscentrallager för databaser, oavsett den specifika teknik, process eller typ av biometriska uppgifter som används. Sådana system för biometrisk fjärridentifiering används vanligtvis för att uppfatta (skanna) flera personer eller deras beteende samtidigt för att avsevärt underlätta identifieringen av ett antal personer utan deras aktiva medverkan. En sådan definition utesluter kontroll- och autentiseringssystem vars enda syfte skulle vara att bekräfta att en viss fysisk person är den person som han eller hon utger sig för att vara, samt system som används för att bekräfta en fysisk persons identitet enbart i syfte att få tillgång till en tjänst, en enhet eller lokaler. Detta uteslutande motiveras av att sådana system sannolikt har en mindre inverkan på fysiska personers grundläggande rättigheter än system för biometrisk fjärridentifiering som kan användas för behandling av biometriska uppgifter om ett stort antal personer. 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 tillhandahålla 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.

(9) I denna förordning bör begreppet allmänt tillgänglig plats förstås som varje fysisk plats som är tillgänglig för ett obestämt antal fysiska personer oberoende av om platsen i fråga är privatägd eller offentligägd och 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 potentiell kapacitet 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.

(10) 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 användare av AI-system som är etablerade i unionen.

(11) Mot bakgrund av AI-systemens digitala natur bör vissa AI-system omfattas av denna förordning även om de varken 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 aktör som är etablerad utanför unionen och entreprenaden avser en aktivitet som ska utföras av ett AI-system som skulle klassificeras som hög risk. Under dessa omständigheter skulle det AI-system som används av aktören utanför unionen kunna behandla data som på lagligt sätt samlats in och överförts från unionen och förse den avtalsslutande aktören 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 den också tillämpas på leverantörer och användare av AI-system som är etablerade i tredjeländer, i den utsträckning som de utdata som produceras av AI-systemen används 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 internationella avtal som ingåtts på nationell eller europeisk nivå och som avser brottsbekämpande och rättsligt samarbete med unionen eller dess medlemsstater. Sådana avtal har ingåtts bilateralt mellan medlemsstater och tredjeländer eller mellan Europeiska unionen, Europol och andra EU-organ och tredjeländer och internationella organisationer. De av mottagarmedlemsstaters myndigheter och unionens institutioner och organ som använder sådana resultat i unionen förblir ansvariga för att se till att deras användning 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.

(12) Denna förordning bör också tillämpas på unionens institutioner, kontor, organ och byråer när de agerar som tillhandahållare eller användare av AI-system.

(-12a) 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 undantas 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 undantag 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 fördraget om Europeiska unionen (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 undantaget både av att den nationella säkerheten förblir medlemsstaternas eget ansvar i enlighet med artikel 4.2 i EU-fördraget och av den nationella säkerhetsverksamhetens särskilda karaktär och operativa behov 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) skulle 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 (dvs. militärt, eller som rör försvar eller nationell säkerhet) som undantas och ett eller flera icke-undantagna ändamål (t.ex. civila ändamål, brottsbekämpning osv.) 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 ändamål som rör 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 brottsbekämpande ändamål 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.

(12a) Denna förordning bör inte påverka tillämpningen av bestämmelserna om tjänstelevererande mellanhänders ansvar enligt Europaparlamentets och rådets direktiv 2000/31/EG [ändrat genom rättsakten om digitala tjänster].

(12b) Denna förordning bör inte underminera forskning och utveckling och den bör respektera forskningsfriheten. Det är därför nödvändigt att från dess tillämpningsområde undanta AI-system som särskilt utvecklats och tagits i bruk enbart för vetenskaplig forskning och utveckling, och att se till att förordningen inte på annat sätt påverkar vetenskaplig forsknings- och utvecklingsverksamhet avseende AI-system. Inte heller när det gäller leverantörernas produktorienterade forskningsverksamhet bör bestämmelserna i denna förordning tillämpas. Detta påverkar inte skyldigheten att följa denna förordning när ett AI-system som omfattas av 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 ovanstående 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 under alla omständigheter genomföras i enlighet med erkända etiska och yrkesmässiga standarder för vetenskaplig forskning.

(12c) Mot bakgrund av karaktären hos och komplexiteten i värdekedjan för AI-system är det viktigt att klargöra rollen för aktörer som kan bidra till utvecklingen av AI-system, särskilt AI-system med hög risk. Det är i synnerhet nödvändigt att klargöra att AI-system för allmänna ändamål är AI-system som av leverantören är avsedda att utföra allmänt tillämpliga funktioner, såsom bild- och taligenkänning, och i en mångfald av sammanhang. De kan användas som AI-system med hög risk själva eller vara komponenter i andra AI-system med hög risk. Därför bör sådana system, på grund av deras särskilda karaktär och för att säkerställa en rättvis ansvarsfördelning längs AI-värdekedjan, omfattas av proportionella och mer specifika krav och skyldigheter enligt denna förordning, samtidigt som en hög nivå av skydd av grundläggande rättigheter, hälsa och säkerhet säkerställs. Dessutom bör leverantörer av AI-system för allmänna ändamål, oavsett om dessa kan användas som AI-system med hög risk som sådana av andra leverantörer eller som komponenter i AI-system med hög risk, på lämpligt sätt samarbeta med leverantörerna av respektive AI-system 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. För att ta hänsyn till särdragen hos AI-system för allmänna ändamål och den snabba utvecklingen på marknaden och den tekniska utvecklingen på området bör kommissionen tilldelas genomförandebefogenheter för att specificera och anpassa tillämpningen av de krav som fastställs enligt denna förordning för AI-system för allmänna ändamål och för att specificera den information som ska delas av leverantörerna av AI-system för allmänna ändamål för att göra det möjligt för leverantörerna av respektive AI-system med hög risk att fullgöra sina skyldigheter enligt denna förordning.

(13) För att säkerställa en konsekvent och hög skyddsnivå för allmänintressen på områdena hälsa, säkerhet och grundläggande rättigheter bör gemensamma bindande normer fastställas för alla AI-system med hög risk. Dessa normer bör vara förenliga med Europeiska unionens stadga om de grundläggande rättigheterna (stadgan) och bör vara icke-diskriminerande och i linje med unionens internationella handelsåtaganden.

(14) För att införa en uppsättning proportionerliga och effektiva 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 metoder för artificiell intelligens, fastställa vissa krav för AI-system med hög risk och skyldigheter för berörda operatörer samt fastställa transparenskrav för vissa AI-system.

(15) Vid sidan av de många nyttiga användningsområdena för artificiell intelligens kan tekniken också missbrukas och tillhandahålla nya och kraftfulla verktyg för manipulation, utnyttjande och social kontroll. Sådana metoder är särskilt skadliga och bör förbjudas eftersom de strider mot unionens värden och respekten för människans värdighet, frihet, jämlikhet, demokrati och rättsstatsprincipen samt unionens grundläggande rättigheter, inbegripet rätten till icke-diskriminering, dataskydd och personlig integritet samt barnets rättigheter.

(16) 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 och ibruktagandet eller användningen av vissa AI-system som väsentligt snedvrider det mänskliga beteendet och som sannolikt kan medföra fysisk eller psykisk skada bör förbjudas. Sådana AI-system använder subliminala komponenter såsom ljud-, bild- och videostimuli som människor inte kan uppfatta eftersom dessa stimuli ligger utanför människans uppfattningsförmåga eller annan subliminal teknik som undergräver eller försämrar människors autonomi, beslutsfattande eller fria val på ett sätt som människor inte är medvetna om eller, även om de är medvetna om detta, inte kan kontrollera eller stå emot, till exempel i fall av gränssnitt mellan en maskin och hjärnan eller virtuell verklighet. Dessutom kan AI-system också på annat sätt utnyttja sårbarheter hos en viss grupp av personer på grund av ålder, funktionsnedsättning i den mening som avses i direktiv (EU) 2019/882 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. 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 fysisk eller psykologisk skada för den personen eller en annan person eller grupper av personer, inbegripet skador som kan ackumuleras över tid. Avsikten att snedvrida beteendet kan inte presumeras om snedvridningen beror på faktorer utanför AI-systemet som ligger utanför leverantörens eller användarens kontroll, vilket innebär faktorer som inte rimligen kan förutses och mildras av leverantören eller användaren av AI-systemet. I vilket fall som helst är det inte nödvändigt att leverantören eller användaren har för avsikt att orsaka den fysiska eller psykiska skadan, så länge sådan skada beror på manipulativ eller utnyttjande AI-baserad teknik. Förbuden mot sådana AI-tillämpningar kompletterar bestämmelserna i direktiv 2005/29/EG, särskilt att otillbörliga affärsmetoder som leder till ekonomisk eller finansiell skada för konsumenterna är förbjudna under alla omständigheter, oavsett om de 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 tillämpliga medicinska normer och lagstiftning. Dessutom bör vanliga och legitima affärsmetoder som är förenliga med tillämplig lagstiftning inte i sig anses utgöra skadliga manipulativa AI-tillämpningar.

(17) AI-system som tillhandahåller offentliga myndigheters 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 på grundval av deras sociala beteende i olika sammanhang eller kända eller förutsedda personliga egenskaper. 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 personernas sociala beteende är. AI-system som medför sådana oacceptabla poängsättningsmetoder bör därför förbjudas. Detta förbud bör inte påverka lagliga metoder för bedömning av fysiska personer som tillämpas för ett eller flera specifika ändamål i enlighet med lagstiftningen.

(18) Användningen av system för biometrisk fjärridentifiering i realtid av fysiska personer på allmänt tillgängliga platser för brottsbekämpningssyften anses särskilt inkräkta 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. De omedelbara effekterna och de begränsade möjligheterna för 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.

(19) 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 potentiella brottsoffer, inklusive försvunna barn, vissa hot mot fysiska personers liv eller fysiska säkerhet eller hot om en terroristattack, Dessa situationer inbegriper sökandet efter potentiella brottsoffer, inklusive försvunna barn, vissa hot mot fysiska personers liv eller fysiska säkerhet eller hot om en terroristattack, och avslöjande, lokalisering, identifiering eller lagföring av gärningsmän till eller misstänkta för brott som avses i rådets rambeslut 2002/584/RIF[9], om dessa brott i den berörda medlemsstaten kan leda till fängelse eller annan frihetsberövande åtgärd för en maxperiod av minst tre år, i enlighet med den medlemsstatens lagstiftning. En sådan tröskel för påföljden i enlighet med nationell lagstiftning bidrar till att säkerställa att brottet är allvarligt nog för att potentiellt motivera användningen av system för biometrisk fjärridentifiering i realtid. Av de 32 brott som finns förtecknade i rådets rambeslut 2002/584/RIF kommer vissa sannolikt 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 avslöjande, lokalisering, identifiering eller lagföring 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. 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 en person 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 skulle till exempel kunna 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.

---

[9] 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) 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 omfattas av lämpliga tids- och platsmässiga begränsningar, med särskild hänsyn till bevis eller indikationer vad gäller hoten, offren eller gärningsmännen. Referensdatabasen över personer bör vara ändamålsenlig för varje användningsfall i var och en av de situationer som anges ovan.

(21) 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 i en medlemsstat. Dessa tillstånd bör i princip erhållas innan systemet används för att identifiera en eller flera personer. Undantag mot denna regel bör tillåtas i vederbörligen motiverade brådskande situationer, alltså situationer då behovet av att använda de berörda systemen är sådant att det i praktiken är objektivt omöjligt att erhålla ett tillstånd innan användningen inleds. I sådana brådskande situationer bör användningen begränsas till det absoluta minimum som är nödvändigt och 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. Den brottsbekämpande myndigheten bör i sådana situationer också sträva efter att erhålla ett tillstånd så snart som möjligt, och även ange skälen till att den inte kunnat ansöka om tillstånd tidigare.

(22) 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.

(23) 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 endast vara möjlig 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 i brottsbekämpande syfte, 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 detta sammanhang är denna förordning inte avsedd att tillhandahålla en rättslig grund för behandling av personuppgifter enligt artikel 8 i direktiv 2016/680. Användningen av system för biometrisk fjärridentifiering i realtid på allmänt tillgänglig plats för andra syften än brottsbekämpning, inbegripet av offentliga myndigheter, bör inte omfattas av den särskilda ram för sådan användning i brottsbekämpningssyfte som fastställs i denna förordning. Sådan användning för andra syften 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 detta.

(24) 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 i syfte att entydigt identifiera en fysisk person, såvida inte någon av situationerna i respektive punkt 2 i dessa två artiklar är tillämplig.

(25) 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 de bestämmelser i artikel 5.1 d, 5.2 5.3 och 5.4 i denna förordning 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 i 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.

(26) 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 bestämmelserna i artikel 5.1 d, 5.2 5.3 och 5.4 i denna förordning 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 kapitlen 4 och 5 i avdelning V i tredje delen av EUF-fördraget.

(27) 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. 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, i förekommande fall.

(28) AI-system skulle kunna producera negativa effekter för personers hälsa och säkerhet, i synnerhet när sådana system fungerar som komponenter i produkter. I enlighet med syftena för unionens harmoniserade lagstiftning, 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. 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, konsumentskydd, arbetstagares rättigheter, rättigheter för personer med funktionsnedsättning, 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 att barn har särskilda rättigheter i enlighet med artikel 24 i EU-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.

(29) 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[10], Europaparlamentets och rådets förordning (EU) nr 167/2013[11], Europaparlamentets och rådets förordning (EU) nr 168/2013[12], Europaparlamentets och rådets direktiv 2014/90/EU[13], Europaparlamentets och rådets direktiv (EU) 2016/797[14], Europaparlamentets och rådets förordning (EU) 2018/858[15], Europaparlamentets och rådets förordning (EU) 2018/1139[16] och Europaparlamentets och rådets förordning (EU) 2019/2144[17], 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 styrelseformer eller mekanismer för kontroll av överensstämmelse och 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 framtida delegerade akter eller genomförandeakter på grundval av dessa akter.

---

10 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).

11 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).

12 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).

13 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).

14 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).

15 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).

16 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).

17 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).

(30) 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.

(31) 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 ”hög risk” enligt de kriterier som fastställs i den relevanta unionslagstiftning om harmonisering som är tillämplig på produkten. Detta gäller i synnerhet för Europaparlamentets och rådets förordning (EU) 2017/745[18] och Europaparlamentets och rådets förordning (EU) 2017/746[19], i vilka tredjepartsbedömning av överensstämmelse föreskrivs för produkter med medelhög risk och hög risk.

[18] 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).

[19] 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).

(32) När det gäller andra AI-system med hög risk än sådana som utgör säkerhetskomponenter i produkter, 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 förordningen. 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. Det är också viktigt att klargöra att det inom de högriskscenarier som avses i bilaga III kan finnas system som inte leder till en betydande risk för de rättsliga intressen som skyddas enligt dessa scenarier, med beaktande av de utdata som AI-systemet producerar. Därför bör det AI-system som genererar sådana utdata betraktas som hög risk endast om dessa utdata har stor betydelse (dvs. inte enbart är accessoriska) med avseende på den berörda åtgärden eller det berörda beslutet genom att skapa en betydande risk för de rättsliga intressen som skyddas. När den information som tillhandahålls av ett AI-system till människan till exempel består av profilering av fysiska personer i den mening som avses i artikel 4.4 i förordning (EU) 2016/679, artikel 3.4 i direktiv (EU) 2016/680 och artikel 3.5 i förordning (EU) 2018/1725, bör sådan information normalt inte anses vara av accessorisk karaktär i samband med AI-system med hög risk enligt bilaga III. Om AI-systemets utdata emellertid endast har försumbar eller mindre relevans för människors agerande eller beslut kan de betraktas som rent accessoriska, inbegripet till exempel AI-system som används för översättning i informationssyfte eller för hantering av dokument.

(33) Tekniska brister i AI-system som är avsedda för biometrisk fjärridentifiering av fysiska personer kan leda till snedvridna resultat och medföra diskriminerande effekter. Detta är särskilt relevant när det gäller ålder, etnicitet, ras, kön eller funktionsnedsättning. Därför bör system för biometrisk fjärridentifiering i realtid och i efterhand klassificeras som hög risk. Mot bakgrund av de risker som dessa system utgör bör båda typerna av system för biometrisk fjärridentifiering omfattas av särskilda krav avseende loggningskapacitet och mänsklig tillsyn.

(34) 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 i direktivet om kritiska entiteters motståndskraft, 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. Vid funktionsavbrott eller funktionsstörning i sådana komponenter kan detta 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 i centrum för molnbaserade datortjänster.

(35) AI-system som används för yrkesutbildning eller annan utbildning, i synnerhet när det gäller fastställandet av personers tillgång eller antagande till institutioner eller program för yrkesutbildning eller annan utbildning på alla nivåer, eller för att utvärdera personers läranderesultat, bör anses som hög risk eftersom de kan avgöra en persons utbildningsväg och yrkeskarriär och därmed påverka deras försörjningsmöjligheter. När sådana system utformas och används på otillbörligt sätt kan de innebära en kränkning av rätten till yrkesutbildning och annan utbildning liksom rätten att inte utsättas för diskriminering eller för en fortsättning på historiska diskrimineringsmönster.

(36) AI-system som används i utbildning, arbetsledning och tillgång till egenföretagande, i synnerhet när det gäller rekrytering eller urval av personer, för beslutsfattande om befordran eller uppsägning och för fördelning av uppgifter grundat på individuellt beteende eller personlighetsdrag och egenskaper, 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 de berörda personerna. Relevanta arbetsrelaterade avtalsförhållanden bör innefatta arbetstagare och personer som tillhandahåller tjänster via plattformar enligt kommissionens arbetsprogram för 2021. Sådana personer bör i princip inte betraktas som användare enligt denna förordning. 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 dessa personers prestation och beteende kan också påverka deras rätt till dataskydd och personlig integritet.

(37) 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 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 detta ändamål kan medföra diskriminering av personer eller grupper eller reproducera historiska diskrimineringsmönster, exempelvis baserat på rasmässigt eller etniskt ursprung, funktionsnedsättning, ålder eller sexuell läggning, eller skapa nya former av diskrimineringseffekter. AI-system för kreditprövning och kreditomdömen bör, när de tas i bruk av mikroföretag eller små företag enligt definitionen i bilagan till kommissionens rekommendation 2003/361/EG för deras eget bruk, undantas mot bakgrund av effekternas mycket begränsade omfattning och de tillgängliga alternativen på marknaden. Fysiska personer som ansöker om eller erhåller väsentliga offentliga bidragsförmåner och tjänster från offentliga myndigheter är normalt beroende av dessa förmåner och tjänster och i en utsatt position i förhållande till de ansvariga myndigheterna. Om AI-system används för att avgöra om sådana förmåner och tjänster ska 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. Dessa system bör därför 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. Slutligen bör även AI-system som används för att sända ut eller fastställa prioriteringsordning för utsändning av larmtjänster klassificeras som hög risk, eftersom dessa system fattar beslut i situationer som är mycket kritiska för personers liv, hälsa och egendom. AI-system används också i allt högre grad för riskbedömning när det gäller fysiska personer och prissättning i fråga om livförsäkringar och sjukförsäkringar som, om de inte utformas, utvecklas och används på rätt sätt, kan få allvarliga konsekvenser för människors liv och hälsa, inbegripet ekonomisk utestängning och diskriminering. För att säkerställa en konsekvent strategi inom sektorn för finansiella tjänster bör det ovannämnda undantaget för mikroföretag eller små företag för egen användning tillämpas, i den mån de själva tillhandahåller och tar i bruk ett AI-system i syfte att sälja sina egna försäkringsprodukter.

(38) Brottsbekämpande myndigheters åtgärder som involverar vissa typer av användning av AI-system kännetecknas 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 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 annat sätt 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 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 de berörda åtgärdernas art och relaterade risker bör dessa AI-system med hög risk i synnerhet inbegripa AI-system avsedda att användas av brottsbekämpande myndigheter för individuella riskbedömningar, lögndetektorer och liknande verktyg för att läsa av en fysisk persons emotionella tillstånd, bedöma tillförlitligheten i bevis i brottmålsförfaranden, förutse förekomsten eller upprepningen av ett faktiskt eller potentiellt brott baserat på profilering av fysiska personer, eller bedöma personlighetsdrag och egenskaper eller tidigare brottsligt beteende hos fysiska personer eller grupper, samt 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 unionslagstiftningen om penningtvätt bör inte anses som AI-system med hög risk som används av brottsbekämpande myndigheter i syfte att förebygga, förhindra, avslöja, utreda eller lagföra brott.

(39) AI-system som används inom förvaltning av migration, asyl och gränskontroll 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, i synnerhet deras rätt till fri rörlighet, icke-diskriminering, skydd av privatliv och personuppgifter, internationellt skydd och god förvaltning. Det är därför lämpligt att som hög risk klassificera AI-system avsedda att användas av behöriga offentliga myndigheter som anförtrotts uppdrag på områdena migration, asyl och gränskontroll, såsom lögndetektorer och liknande verktyg för att läsa av en fysisk persons emotionella tillstånd, för bedömning av vissa risker som utgörs av fysiska personer som reser in till en medlemsstats territorium eller som ansöker om visum eller asyl, och för att bistå behöriga offentliga myndigheter i granskningen av ansökningar om asyl, visum och uppehållstillstånd och därmed förbundna klagomål med avseende på syftet att fastställa om den ansökande fysiska personen uppfyller kraven för denna status. AI-system på området migration, asyl och gränskontroll vilka omfattas av denna förordning bör uppfylla de relevanta förfarandemässiga krav som fastställs i Europaparlamentets och rådets direktiv 2013/32/EU[20], Europaparlamentets och rådets förordning (EG) nr 810/2009[21] och annan relevant lagstiftning.

[20] 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).

[21] 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).

(40) 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 hjälpa de rättsliga myndigheterna att tolka fakta och lagstiftning och att tillämpa denna lagstiftning på en konkret uppsättning fakta. Denna kategorisering 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.

(41) Det faktum att ett AI-system klassificerats som hög risk enligt denna förordning bör inte tolkas som att användningen av det systemet är laglig enligt andra rättsakter i unionsrätten eller enligt nationell lagstiftning 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 uttryckligen annat föreskrivs i denna förordning.

(42) För att begränsa riskerna med AI-system med hög risk som släpps ut eller på annat sätt tas i bruk på unionsmarknaden bör vissa obligatoriska krav gälla, med beaktande av systemets avsedda ändamål eller användning och i enlighet med det riskhanteringssystem som ska upprättas av leverantören. Riskhanteringssystemet bör särskilt bestå av en kontinuerlig iterativ process som planeras och löper under hela livscykeln för ett AI-system med hög risk. Denna process bör säkerställa att leverantören identifierar och analyserar riskerna för hälsa, säkerhet och grundläggande rättigheter för de personer som kan påverkas av systemet mot bakgrund av dess avsedda ändamål, inbegripet de eventuella risker som uppstår till följd av interaktionen mellan AI-systemet och den miljö där det är verksamt, och följaktligen antar lämpliga riskhanteringsåtgärder mot bakgrund av teknikens ståndpunkt.

(43) Kraven bör tillämpas på AI-system med hög risk när det gäller kvaliteten på använda dataset, teknisk dokumentation och arkivering, transparens och information till användarna, 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, såsom tillämpligt mot bakgrund av systemets avsedda syfte, och om inga andra åtgärder som är mindre handelsbegränsande finns rimligen tillgängliga, för att på så sätt motverka omotiverade begränsningar av handeln.

(44) Data av hög kvalitet krävs för 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 till en källa till diskriminering som är förbjuden enligt unionsrätten. För högkvalitativ träning, validering och testning av dataset krävs genomförandet av ändamålsenliga metoder för dataförvaltning och datahantering. Tränings-, validerings- och testningsdataset bör vara tillräckligt relevanta och representativa samt ha lämpliga statistiska egenskaper, inbegripet vad gäller de personer eller grupper av personer på vilka AI-systemet med hög risk är avsett att användas. Dessa dataset bör också vara så felfria och fullständiga som möjligt med tanke på AI-systemets avsedda ändamål, med beaktande, på ett proportionellt sätt, den tekniska genomförbarheten och teknikens ståndpunkt, tillgången till data och genomförandet av lämpliga riskhanteringsåtgärder så att eventuella brister i datauppsättningarna åtgärdas på vederbörligt sätt. Kravet på att dataseten ska vara fullständiga och felfria bör inte påverka användningen av integritetsbevarande teknik i samband med utveckling och testning av AI-system. Tränings-, validerings- och testningsdataset bör, i den mån som krävs för deras avsedda ändamål, beakta funktioner, särdrag eller element som är specifika för den särskilda geografiska, beteendemässiga eller funktionsmässiga situation eller kontext där AI-systemet är avsett att användas. För att skydda andras rätt att slippa diskriminering som kan följa av snedvridning i AI-system, bör leverantörerna kunna behandla även särskilda kategorier av personuppgifter, som en fråga av viktigt allmänt intresse 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, för att säkerställa övervakning, upptäckt och korrigering av snedvridning när det gäller AI-system med hög risk.

(44a) Vid tillämpningen av de principer som avses i artikel 5.1 c i förordning (EU) 2016/679 och artikel 4.1 c i förordning (EU) 2018/1725, särskilt principen om uppgiftsminimering, när det gäller tränings-, validerings- och testningsdataset enligt denna förordning, bör vederbörlig hänsyn tas till AI-systemets hela livscykel.

(45) För utvecklingen av AI-system med hög risk bör vissa aktörer, såsom leverantörer, anmälda organ och andra berörda enheter – exempelvis digitala innovationsknutpunkter, test- och försöksanläggningar 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 det offentliga i allmänhetens intresse kommer att vara avgörande för tillhandahållandet av förtroendebaserad, 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 algoritmer för artificiell intelligens med användning av 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.

(46) Det är mycket viktigt att ha information om hur AI-system med hög risk har utvecklats och hur de utför sina funktioner under hela sin livscykel, för att kontrollera att kraven enligt denna förordning uppfylls. Detta förutsätter arkivering och tillgång till teknisk dokumentation som innehåller den information som krävs för att bedöma om AI-systemet uppfyller de berörda kraven. Denna information bör innefatta systemets allmänna egenskaper, förmågor och begränsningar samt algoritmer, data, träning, de förfaranden som används för testning och validering samt dokumentation av relevanta riskhanteringssystem. Den tekniska dokumentationen bör vara uppdaterad. Dessutom bör leverantörer eller användare spara loggar som genereras automatiskt av AI-systemet med hög risk, inbegripet till exempel utdata, startdatum och starttid osv., i den mån detta system och tillhörande loggar står under deras kontroll, under en period som är lämplig för att göra det möjligt för dem att fullgöra sina skyldigheter.

(47) I och med att vissa AI-system kan vara så svårgenomträngliga att de blir obegripliga eller för komplexa för fysiska personer bör en viss grad av transparens krävas för AI-system med hög risk. Användarna bör kunna tolka systemets utdata och använda dessa på lämpligt sätt. AI-system med hög risk bör därför åtföljas av relevant dokumentation och bruksanvisning och innefatta koncis och tydlig information, däribland vad gäller möjliga risker för grundläggande rättigheter och diskriminering av de personer som kan påverkas av systemet mot bakgrund av dess avsedda ändamål, när så är lämpligt. För att göra det lättare för användarna att förstå bruksanvisningen bör de innehålla belysande exempel på lämpligt sätt.

(48) AI-system med hög risk bör utformas och utvecklas på ett sådant sätt att fysiska personer kan övervaka deras funktionssätt. 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. 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 användaren 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 skulle kunna 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 skulle kunna vara tillräckligt att de olika personernas separata kontroller automatiskt registreras i de loggar som genereras av systemet.

(49) AI-system med hög risk bör fungera konsekvent under hela sin livscykel och uppnå en lämplig nivå av noggrannhet, robusthet och cybersäkerhet i enlighet med den allmänt erkända bästa tekniken. Användarna bör informeras om graden av noggrannhet och om mätningen av noggrannheten.

(50) 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). AI-system med hög risk bör därför utformas och utvecklas med lämpliga tekniska lösningar för att förebygga eller minimera sådant skadligt eller på annat sätt oönskat beteende, till exempel 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.

(51) Cybersäkerhet har en viktig roll för att säkerställa att AI-systemen är resilienta mot försök att ändra deras användning, beteende eller prestanda eller att undergräva deras säkerhetsegenskaper genom illasinnade tredje parter som utnyttjar systemets svagheter. Cyberattacker mot AI-system kan riktas mot AI-specifika tillgångar, såsom kollektioner av träningsdata (s.k. dataförgiftning) eller algoritmerna som använder dessa data (såsom mjukvaruhacking eller antagonistiska exempel), 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 lämpliga åtgärder därför vidtas av leverantörerna av AI-system med hög risk, även med beaktande av den underliggande IKT-infrastrukturen, när så är lämpligt.

(52) Som ett led i unionens lagstiftning om harmonisering bör regler som är tillämpliga på utsläppande på marknaden, ibruktagandet och användningen av AI-system med hög risk fastställas i enlighet med Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter[22], Europaparlamentets och rådets beslut nr 768/2008/EG om en gemensam ram för saluföring av produkter[23] samt Europaparlamentets och rådets förordning (EU) 2019/1020 om marknadskontroll och överensstämmelse för produkter[24] (*den nya lagstiftningsramen*).

(52a) I linje med den nya lagstiftningsramens principer bör särskilda skyldigheter fastställas för berörda operatörer inom AI-värdekedjan, för att säkerställa rättssäkerheten och underlätta efterlevnaden av denna förordning. I vissa situationer skulle dessa operatörer kunna agera i mer än en roll samtidigt och bör därför kumulativt fullgöra alla relevanta skyldigheter med anknytning till dessa roller. En operatör skulle till exempel samtidigt kunna agera som distributör och importör.

(53) Det är lämpligt att en specifik fysisk eller juridisk person, definierad som leverantören, tar ansvaret för utsläppandet på marknaden eller ibruktagandet av AI-system med hög risk, oavsett om denna fysiska eller juridiska person är den person som utformat eller utvecklat systemet.

---

22 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).

23 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).

24 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).

(54) Leverantören bör inrätta ett sunt kvalitetsledningssystem, säkerställa att föreskrivna förfaranden för bedömning av överensstämmelse genomförs, utarbeta den relevanta dokumentationen och inrätta ett robust system för övervakning efter utsläppandet på marknaden. Offentliga myndigheter som för egen användning tar i bruk AI-system med hög risk får anta och genomföra reglerna för kvalitetsledningssystemet som en del av det kvalitetsledningssystem som införs på nationell eller regional nivå, såsom lämpligt, med beaktande av sektorns särdrag och den berörda offentliga myndighetens kompetensområde och organisation.

(54a) För att säkerställa rättssäkerhet är det nödvändigt att klargöra att under vissa särskilda villkor bör varje fysisk eller juridisk person betraktas som leverantör av ett nytt AI-system med hög risk och därför åta sig alla relevanta skyldigheter. Detta skulle till exempel vara fallet om den personen sätter sitt namn eller varumärke på ett AI-system med hög risk som redan släppts ut på marknaden eller tagits i bruk, eller om den personen ändrar det avsedda ändamålet med ett AI-system som inte är ett högrisksystem och som redan släppts ut på marknaden eller tagits i bruk, på ett sätt som gör det ändrade systemet till ett AI-system med hög risk. Dessa bestämmelser bör tillämpas utan att det påverkar tillämpningen av mer specifika bestämmelser som fastställs i viss sektorsspecifik lagstiftning inom 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 skulle kunna 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.

(55) I de fall då ett AI-system med hög risk som ingår som säkerhetskomponent i en produkt som omfattas av relevant sektorslagstiftning inom den nya lagstiftningsramen inte släpps ut på marknaden och inte heller tas i bruk fristående från produkten, bör produkttillverkaren, enligt definitionen i den relevanta lagstiftningen inom den nya lagstiftningsramen, 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.

(56) För att möjliggöra kontroll av efterlevnaden av denna förordning och säkerställa lika villkor för aktörerna, och med beaktande av de olika formerna för att göra digitala produkter tillgängliga, är det viktigt att säkerställa att en person som är etablerad i unionen under alla omständigheter kan förse myndigheterna med all den informationen om AI-systemens överensstämmelse som är nödvändig. Innan leverantörer etablerade utanför unionen gör sina AI-system tillgängliga i unionen bör de, i de fall då ingen importör kan identifieras, genom skriftlig fullmakt utse ett ombud i unionen.

(56a) I fråga om leverantörer som inte är etablerade i unionen har ombudet en central roll som garant för att de AI-system med hög risk som släpps ut på marknaden eller tas i bruk av dessa leverantörer uppfyller kraven och som tillverkarnas kontaktpersoner etablerade i unionen. Med tanke på denna centrala roll, och för att säkerställa att ansvaret tas i samband med efterlevnaden av denna förordning, är det lämpligt att göra ombudet solidariskt ansvarig med leverantören för AI-system med hög risk som har säkerhetsbrister. Det ansvar för ombudet som föreskrivs i denna förordning påverkar inte tillämpningen av bestämmelserna i direktiv 85/374/EEG om skadeståndsansvar för produkter med säkerhetsbrister.

(57) [utgår]

(58) 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 användarna. Användarna bör i synnerhet använda AI-system med hög risk i enlighet med bruksanvisningarna, och vissa andra skyldigheter bör föreskrivas när det gäller övervakning av AI-systemens funktionssätt och arkivering, såsom lämpligt. Dessa skyldigheter bör inte påverka andra användarskyldigheter i samband med AI-system med hög risk enligt unionsrätten eller nationell rätt, och bör inte gälla om användningen sker inom ramen för en personlig icke-yrkesmässig verksamhet.

(58a) Det är lämpligt att klargöra att denna förordning inte påverkar de skyldigheter som leverantörer och användare av AI-system har i sin roll som personuppgiftsansvariga eller personuppgiftsbiträden enligt unionsrätten 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.

(59) [utgår]

(60) [utgår]

(61) Standardisering bör ha en nyckelroll för att förse leverantörerna med tekniska lösningar för att säkerställa efterlevnaden av denna förordning i linje med teknikens ståndpunkt. Överenstämmelse med harmoniserade standarder enligt Europaparlamentets och rådets förordning (EU) nr 1025/2012[25], som normalt förväntas återspegla teknikens ståndpunkt, bör vara ett sätt för leverantörerna att visa att de uppfyller kraven i denna förordning. I avsaknad av relevanta hänvisningar till harmoniserade standarder bör kommissionen dock genom genomförandeakter kunna fastställa gemensamma specifikationer för vissa krav enligt denna förordning som en undantagslösning för att underlätta leverantörens skyldighet att uppfylla kraven i denna förordning, när standardiseringsprocessen blockeras eller när fastställandet av en lämplig harmoniserad standard försenas. Om en sådan försening beror på den tekniska komplexiteten hos standarden i fråga bör kommissionen överväga detta innan man överväger att fastställa gemensamma specifikationer. Ett lämpligt deltagande av små och medelstora företag i utarbetandet av standarder till stöd för genomförandet av denna förordning är avgörande för att främja innovation och konkurrenskraft på området artificiell intelligens i unionen. Ett sådant deltagande bör säkerställas på lämpligt sätt i enlighet med artiklarna 5 och 6 i förordning (EG) nr 1025/2012.

[25] 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 nr 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

(61a) Utan att det påverkar användningen av harmoniserade standarder och gemensamma specifikationer, bör leverantörer omfattas av en presumtion om överensstämmelse med det relevanta kravet på data när deras AI-system med hög risk har tränats och testats på data som återspeglar den specifika geografiska, beteendemässiga eller funktionella miljö inom vilken AI-systemet är avsett att användas. I enlighet med artikel 54.3 i Europaparlamentets och rådets förordning (EU) 2019/881, bör på samma sätt AI-system med hög risk, som har certifierats eller för vilka en försäkran om överensstämmelse har utfärdats inom ramen för en ordning för cybersäkerhet i enlighet med den förordningen och till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning*, förutsättas överensstämma med cybersäkerhetskravet i denna förordning. Detta påverkar inte den frivilliga karaktären hos denna ordning för cybersäkerhet.

(62) 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.

(63) För att minimera bördan för aktörerna och motverka allt eventuellt dubbelarbete är det, för AI-system med hög risk som är relaterade till produkter som omfattas av befintlig unionslagstiftning om harmonisering som följer av den nya lagstiftningsramens metod, 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 lagstiftningen inom den nya lagstiftningsramen. Detta tillvägagångssätt beaktas helt i samspelet mellan denna förordning och [maskinförordningen]. Denna förordning behandlar säkerhetsriskerna med AI-system som säkerställer säkerhetsfunktioner i maskiner, medan vissa särskilda krav i [maskinförordningen] kommer att säkerställa en säker integrering av AI-system i maskinerna som helhet, för att inte undergräva deras övergripande säkerhet. I [maskinförordningen] gäller samma definition av AI system som i denna förordning. När det gäller AI-system med hög risk som är relaterade till produkter som omfattas av förordningarna (EU) 2017/745 och (EU) 2017/746 om medicintekniska produkter bör tillämpligheten av kraven i denna förordning inte påverka men beakta den riskhanteringslogik och bedömning av nytta-risk-förhållandet som utförs inom ramen för den medicintekniska produkten.

(64) Mot bakgrund av den mer omfattande erfarenheten av professionella certifieringsorgan före utsläppandet på marknaden på området produktsäkerhet och de olika typer av risker som är involverade, är det 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 de som är relaterade till produkter. Därför bör bedömningen av överensstämmelse för sådana system som allmän regel utföras av leverantören under dennes eget ansvar, med det enda undantaget att ett anmält organs deltagande i bedömningen av överensstämmelse bör föreskrivas för AI-system avsedda att användas för biometrisk fjärridentifiering av personer, i den utsträckning som dessa system inte är förbjudna.

(65) För genomförandet av tredjepartsbedömningen av överensstämmelse för AI-system avsedda att användas för biometrisk fjärridentifiering av personer, 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 och avsaknad av intressekonflikter. 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 beslut 768/2008.

(66) I linje med det vedertagna begreppet väsentlig ändring som avser produkter som regleras genom unionens lagstiftning om harmonisering, är det lämpligt att AI-systemet anses vara ett nytt AI-system som bör genomgå en ny bedömning av överensstämmelse vid varje ändring som kan påverka överensstämmelsen för ett AI -system med hög risk med denna förordning (t.ex. en ändring av operativsystem eller programvaruarkitektur) eller när systemets avsedda ändamål ändras. 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 sitt sätt att utföra funktionerna) bör dock inte utgöra väsentliga ändringar, förutsatt att dessa ändringar har förutbestämts av leverantören och bedömts i samband med bedömningen av överensstämmelse.

(67) AI-system med hög risk bör vara försedda med en CE-märkning som visar att de överensstämmer med denna förordning, så att de omfattas av den fria rörligheten på den inre marknaden. Medlemsstaterna bör inte sätta upp omotiverade hinder för utsläppandet på marknaden eller ibruktagandet av AI-system som uppfyller kraven i denna förordning och är försedda med en CE-märkning.

(68) Under vissa omständigheter kan en snabb tillgång till innovativ teknik vara avgörande för hälsan och säkerheten för personer och för samhället som helhet. Det är därför lämpligt att medlemsstaterna, när det föreligger exceptionella skäl förbundna med allmän säkerhet eller skydd av fysiska personers liv och hälsa och skydd av industriell och kommersiell äganderätt, har möjlighet att tillåta utsläppandet på marknaden eller ibruktagandet av AI-system som inte har genomgått en bedömning av överensstämmelse.

(69) För att underlätta kommissionens och medlemsstaternas arbete på området artificiell intelligens och öka transparensen gentemot allmänheten, bör leverantörer av andra AI-system med hög risk än de som är relaterade till produkter som faller inom tillämpningsområdet för relevant befintlig unionslagstiftning om harmonisering åläggas att registrera sig och information om sina AI-system med hög risk i en EU-databas, som upprättas och förvaltas av kommissionen. Innan ett AI-system med hög risk som förtecknas i bilaga III används ska användare av AI-system med hög risk som är offentliga myndigheter, byråer eller organ, med undantag för brottsbekämpande myndigheter, gränskontrollmyndigheter, immigrations- eller asylmyndigheter och myndigheter som använder AI-system med hög risk på området kritisk infrastruktur, också registrera sig i en sådan databas och välja det system som de planerar att använda. Kommissionen bör vara personuppgiftsansvarig för denna databas i enlighet med Europaparlamentets och rådets förordning (EU) 2018/1725[26]. För att säkerställa att databasen är fullt funktionell när den börjar användas, bör förfarandet för inrättandet av databasen innefatta funktionsspecifikationer som utarbetas av kommissionen samt en oberoende revisionsrapport.

[26] 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).

(70) 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. 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 personer som tillhör utsatta grupper på grund av deras ålder eller funktionsnedsättning beaktas i den mån AI-systemet även är avsett att interagera även 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 eller andra aspekter såsom sexuell eller politisk läggning. Sådan information och sådana meddelanden bör tillhandahållas i format som är tillgängliga för personer med funktionsnedsättning. Vidare bör användare 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, upplysa om att innehållet har skapats artificiellt eller manipulerats genom märkning av det innehåll som producerats med artificiell intelligens och upplysa om innehållets artificiella ursprung. Fullgörandet av de informationsskyldigheter som avses ovan 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 användare av AI-system som fastställs i unionsrätten eller nationell rätt. Det bör inte heller tolkas som att användningen av systemet eller dess utdata hindrar rätten till yttrandefrihet och konstens och vetenskapens frihet, som garanteras i Europeiska unionens stadga om de grundläggande rättigheterna, särskilt när innehållet ingår i ett uppenbart kreativt, satiriskt, konstnärligt eller fiktivt verk eller program, med förbehåll för lämpliga garantier för tredje mans rättigheter och friheter.

(71) Artificiell intelligens är en teknikfamilj i snabb utveckling som kräver nya former av tillsyn och ett säkert område för experiment, med säkerställande av ansvarsfull innovation och integrering av ändamålsenliga skydds- och riskbegränsningsåtgärder. För att säkerställa en rättslig ram som är innovationsvänlig, framtidssäkrad och resilient mot störningar, bör de nationella behöriga myndigheterna från en eller flera medlemsstater uppmuntras att inrätta ”regulatoriska sandlådor” för artificiell intelligens, för att främja utveckling och testning av innovativa AI-system under strikt tillsyn innan dessa system släpps ut på marknaden eller på annat sätt tas i bruk.

(72) Syftet med de regulatoriska sandlådorna för AI bör vara att främja AI-innovation genom skapande av en kontrollerad försöks- och testmiljö för utveckling i fasen före utsläppandet på marknaden, med sikte på att säkerställa att de innovativa AI-systemen är förenliga med denna förordning och annan lagstiftning på unions- eller medlemsstatsnivå, att öka rättssäkerheten för innovatörer och förbättra de behöriga myndigheternas tillsyn och förståelse av möjligheterna, de nya riskerna och effekterna av AI-användningen, samt att öka tillgången till marknader, bland annat genom att undanröja hinder 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. 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, innovationsnav och relevanta organisationer för berörda parter och 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 lagstiftning 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.

(-72a) Denna förordning bör erbjuda den rättsliga grunden för att deltagare i den regulatoriska sandlådan för AI använder personuppgifter som samlats in för andra ändamål än för att utveckla vissa AI-system i allmänhetens intresse inom regulatoriska sandlådor för AI, i linje med artikelartiklarna 6.4 och 9.2 g i förordning (EU) 2016/679 och artiklarna 5 och 10 i förordning (EU) 2018/1725, och utan att det påverkar tillämpningen av artikel 4.2 i direktiv (EU) 2016/680. Alla andra skyldigheter för personuppgiftsansvariga och de registrerades rättigheter enligt förordning (EU) 2016/679, förordning (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. Deltagarna 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 begränsa eventuella höga risker för säkerhet och grundläggande rättigheter som kan uppstå i samband med utvecklings- och försöksverksamhet i sandlådan. Deltagarnas agerande i sandlådan bör beaktas när de behöriga myndigheterna beslutar om påförande av administrativa sanktionsavgifter enligt artikel 83.2 i förordning 2016/679 och artikel 57 i direktiv 2016/680.

(72a) För att påskynda utvecklingen och utsläppandet på marknaden av AI-system med hög risk som förtecknas i bilaga III 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 förordningen 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 i fall där 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.

(73) För att främja och skydda innovation är det viktigt att särskild hänsyn tas till sådana leverantörer och användare av AI-system som är små och medelstora företag. I detta syfte bör medlemsstaterna ta fram initiativ som riktar sig till dessa aktörer, bland annat vad gäller medvetandehöjande och information. De särskilda intresse som leverantörer som är små och medelstora företag har bör också beaktas när de anmälda organen fastställer avgifterna för bedömning av överensstämmelse. Kostnaderna för översättning av obligatorisk dokumentation och kommunikation med myndigheter kan utgöra betydande kostnader för leverantörer och andra aktörer, i synnerhet mer småskaliga sådana. Medlemsstaterna bör eventuellt säkerställa att ett av de språk som fastställs och godtas av dem för relevant dokumentation från aktörer och för kommunikation med aktörer är ett språk som i huvudsak förstås av största möjliga antal användare i gränsöverskridande situationer.

(73a) För att främja och skydda innovation bör plattformen för efterfrågestyrd AI, alla relevanta unionsfinansieringsprogram och unionsprojekt, såsom programmet för ett digitalt Europa och Horisont Europa, som genomförs av kommissionen och medlemsstaterna på nationell nivå eller unionsnivå bidra till att målen i denna förordning uppnås.

(74) 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, och de anmälda organens uppfyllande av sina skyldigheter enligt denna förordning, bör plattformen för efterfrågestyrd AI, de europeiska digitala innovationsknutpunkterna och de test- och försöksanläggningar som inrättas av kommissionen och medlemsstaterna på nationell nivå och EU-nivå i synnerhet bidra till genomförandet av denna förordning. Inom sina respektive uppdrag och kompetensområden kan de i synnerhet tillhandahålla tekniskt och vetenskapligt stöd till leverantörer och anmälda organ.

(74a) För att säkerställa proportionalitet med tanke på vissa operatörers mycket små storlek när det gäller innovationskostnader bör dessutom mikroföretag undantas från de mest kostsamma skyldigheterna, såsom att inrätta ett kvalitetsstyrningssystem som skulle minska den administrativa bördan och kostnaderna för dessa företag utan att påverka skyddsnivån och behovet av efterlevnad av kraven för AI-system med hög risk.

(75) 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 unionens lagstiftning om harmonisering. Detta gäller i synnerhet för expertpaneler, expertlaboratorier och referenslaboratorier på området medicintekniska produkter i enlighet med förordning (EU) 2017/745 och förordning (EU) 2017/746.

(76) För att främja ett smidigt, effektivt och harmoniserat genomförande av denna förordning bör en europeisk nämnd för artificiell intelligens inrättas. Nämnden bör återspegla AI-ekosystemets olika intressen och bestå av företrädare för medlemsstaterna. För att säkerställa relevanta berörda parters deltagande bör en ständig arbetsgrupp för nämnden inrättas. 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 efterlevnadsfrågor, 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 artificiell intelligens. För att ge medlemsstaterna viss flexibilitet när de utser sina företrädare i AI-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 linje med kommissionens roll och uppgifter enligt artikel 33 i förordning (EU) 2019/1020 bör kommissionen stödja den verksamheten i den ständiga arbetsgruppens 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 kan inrätta andra ständiga eller tillfälliga arbetsgrupper 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 unionsreglering av data, digitala produkter och tjänster.

(76a) Kommissionen bör aktivt stödja medlemsstaterna och operatörerna i genomförandet och efterlevnaden av denna förordning. I detta avseende bör den utarbeta riktlinjer om särskilda frågor som syftar till att underlätta tillämpningen av denna förordning, samtidigt som särskild uppmärksamhet ägnas åt behoven hos små och medelstora företag och nystartade företag i de sektorer som mest sannolikt kommer att påverkas. För att stödja adekvat efterlevnad och medlemsstaternas kapacitet bör unionsprovningsanläggningar för AI och en pool av relevanta experter inrättas och göras tillgängliga för medlemsstaterna.

(77) EU-länderna har en central roll i tillämpningen och kontrollen av efterlevnaden av denna förordning. I detta hänseende bör varje medlemsstat utse en eller flera nationella behöriga myndigheter för att övervaka tillämpningen och genomförandet av denna förordning. Medlemsstaterna kan besluta att utse varje 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.

(78) 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 ett system för övervakning av produkter som släppts ut på marknaden. 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.

(79) För att säkerställa en ändamålsenlig och effektiv kontroll av uppfyllandet av de krav och skyldigheter som fastställs i denna förordning, som utgör en del av unionens harmoniseringslagstiftning, 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 tillsynsbefogenheter enligt denna förordning och förordning (EU) 2019/1020 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 marknadskontrollmyndigheterna 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.

(79a) 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 ett adekvat och snabb verkställighet mot 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, förbjudna system som har släppts ut på marknaden, tagits i bruk eller använts i strid med det förbud av metoder som fastställs i denna förordning och AI-system som har gjorts tillgängliga i strid med de transparenskrav som fastställs i denna förordning och som utgör en risk.

(80) Unionslagstiftningen om finansiella tjänster omfattar regler och krav för interna styrelseformer och riskhantering som är tillämpliga på reglerade finansiella institut 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 unionslagstiftningen för finansiella tjänster, bör de myndigheter som ansvarar för tillsynen och kontrollen av efterlevnaden av lagstiftningen om finansiella tjänster 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 finansiella institut, såvida inte medlemsstaterna beslutar att utse en annan myndighet att utföra dessa marknadskontrolluppgifter. Dessa behöriga myndigheter bör ha alla befogenheter enligt denna förordning och förordning (EU) 2019/1020 om marknadskontroll för att genomdriva kraven och skyldigheterna i denna förordning, inbegripet befogenheter att utföra vår efterhandskontroll av marknaden som, när så är lämpligt, kan integreras i deras befintliga tillsynsmekanismer och tillsynsförfaranden enligt relevant unionslagstiftning 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 (SSM) som inrättats genom rådets förordning (EU) nr 1024/2013, 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. För att ytterligare öka konsekvensen mellan denna förordning och de regler som är tillämpliga på kreditinstitut som regleras genom Europaparlamentets och rådets direktiv 2013/36/EU[27] 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 kvalitetsledningssystem och de övervakningsskyldigheter som gäller för användare av AI-system med hög risk i den utsträckning som dessa är tillämpliga på kreditinstitut som

[27] 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).

regleras genom direktiv 2013/36/EU. Samma ordning bör tillämpas på försäkrings- och återförsäkringsföretag och försäkringsholdingbolag enligt direktiv 2009/138/EU (Solvens II) och försäkringsförmedlare enligt direktiv (EU) 2016/97 och andra typer av finansiella institut som omfattas av krav avseende interna styrelseformer, arrangemang eller processer som inrättats i enlighet med relevant unionslagstiftning om finansiella tjänster för att säkerställa enhetlighet och likabehandling inom finanssektorn.

(81) 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 tillförlitlig artificiell intelligens i unionen. Leverantörer av AI-system som inte utgör hög risk bör uppmuntras att ta fram uppförandekoder avsedda att främja en frivillig tillämpning av de krav som gäller för AI-system med hög risk, anpassade med hänsyn till systemens avsedda ändamål och den lägre risk som de medför. Leverantörerna bör också uppmuntras att på frivillig grund tillämpa ytterligare krav avseende exempelvis miljömässig hållbarhet, tillgänglighet för personer med funktionsnedsättning, berörda parters deltagande i utformningen och utvecklingen av AI-system samt mångfald i utvecklingsteamen. 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.

(82) Det är viktigt att AI-system som avser produkter som inte utgör hög risk enligt denna förordning och som därmed inte måste uppfylla kraven i förordningen ändå är säkra när de släpps ut på marknaden eller tas i bruk. För att bidra till detta mål skulle Europaparlamentets och rådets direktiv 2001/95/EG[28] tillämpas som ett skyddsnät.

(83) 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 respektera konfidentialiteten för information och data som de erhåller i utförandet av sina uppgifter i enlighet med unionslagstiftningen eller nationell lagstiftning.

---

[28] Europaparlamentets och rådets direktiv 2001/95/EG av den 3 december 2001 om allmän produktsäkerhet (EGT L 11, 15.1.2002, s. 4).

(84) 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, och med iakttagande av principen *ne bis in idem*. För vissa specifika överträdelser bör medlemsstaterna beakta de marginaler och kriterier som fastställs i denna förordning. Europeiska datatillsynsmannen bör ha befogenhet att ålägga böter för unionens institutioner, byråer och organ som omfattas av denna förordning.

(85) 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 unionens harmoniseringslagstiftning som förtecknas i bilaga II, AI-system med hög risk som förtecknas i bilaga III, bestämmelserna om teknisk dokumentation som förtecknas i bilaga IV, innehållet i EU-försäkran om överensstämmelse i bilaga V, bestämmelserna om förfaranden för bedömning av överensstämmelse i bilagorna VI och VII och 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. 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[29]. 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. Sådana samråd och sådant rådgivningsstöd bör också genomföras inom ramen för AI-nämndens och dess arbetsgruppers verksamhet.

[29] EUT L 123, 12.5.2016, s. 1.

(86) 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[30]. Det är särskilt viktigt att kommissionen i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning, när mer omfattande sakkunskap behövs för ett tidigt utarbetande av utkast till genomförandeakter, använder sig av expertgrupper, samråder med berörda parter eller genomför offentliga samråd, beroende på vad som är lämpligt. Sådana samråd och sådant rådgivningsstöd bör också genomföras inom ramen för AI-nämndens och dess arbetsgruppers verksamhet, även vid utarbetande av genomförandeakter som rör artiklarna 4, 4b och 6.

(87) Eftersom målet för denna förordning 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.

(87a) 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, endast om dessa system från och med den dagen genomgår betydande ändringar av sin konstruktion eller sitt avsedda ändamål. Det är lämpligt att klargöra att begreppet betydande ändring i detta avseende bör tolkas som att det i sak motsvarar begreppet väsentlig ändring, som endast används med avseende på AI-system med hög risk enligt definitionen i denna förordning.

---

[30] 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).

(88) Denna förordning bör tillämpas från och med den … [*Publikationsbyrån: för in det datum som fastställs i artikel 85*]. Infrastrukturen för styrning och systemet för bedömning av överensstämmelse bör dock vara operativa före det datumet, därför bör bestämmelserna om anmälda organ och styrningsstruktur tillämpas från och med den … [*Publikationsbyrån: för in datumet – tre månader från denna förordnings ikraftträdande*]. 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 [*Publikationsbyrån: för in datumet – tolv månader från denna förordnings ikraftträdande*].

(89) Europeiska datatillsynsmannen och Europeiska dataskyddsstyrelsen har hörts i enlighet med artikel 42.2 i förordning (EU) nr 2018/1725 och avgav ett yttrande den […]”.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

AVDELNING I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll

I denna förordning fastställs

a) harmoniserade regler för utsläppande på marknaden, ibruktagande och användning av system med artificiell intelligens (*AI-system*) i unionen,

a) förbud mot vissa tillämpningar av artificiell intelligens,

b) särskilda krav för AI-system med hög risk och skyldigheter för operatörer av sådana system,

c) harmoniserade transparensregler för vissa AI-system,

d) regler om marknadskontroll, marknadsövervakning och styrning,

e) åtgärder till stöd för innovation.

Artikel 2

Tillämpningsområde

1. Denna förordning ska tillämpas på

a) leverantörer som släpper ut AI-system på marknaden eller tar AI-system i bruk i unionen, oavsett om dessa leverantörer är fysiskt närvarande eller etablerade i unionen eller i ett tredjeland,

b) användare av AI-system som är fysiskt närvarande eller etablerade i unionen,

c) leverantörer och användare av AI-system som är fysiskt närvarande eller etablerade i ett tredjeland, om de utdata som produceras av 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 är etablerade 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 II ska endast artikel 84 i denna förordning tillämpas: Artikel 53 ska tillämpas endast i den mån som kraven för AI-system med hög risk enligt denna förordning har integrerats i unionens harmoniseringslagstiftning.

3. 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 av sådana system för verksamhet som inte omfattas av unionsrätten, och under alla omständigheter verksamhet som rör militär, försvar eller nationell säkerhet, oavsett vilken typ av enhet som bedriver denna verksamhet.

   Dessutom ska denna förordning inte tillämpas på AI-system som inte släpps ut på marknaden eller tas i bruk i unionen, om utdata används i unionen för verksamhet som inte omfattas av unionsrätten, och under alla omständigheter verksamhet som rör militär, försvar eller 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 internationella avtal om brottsbekämpning och rättsligt samarbete med unionen eller med en eller flera medlemsstater.

5. Denna förordning ska inte påverka tillämpningen av bestämmelserna om tjänstelevererande mellanhänders ansvar i kapitel II avsnitt 4 i Europaparlamentets och rådets direktiv 2000/31/EG[31] [*som ska ersättas av motsvarande bestämmelser i rättsakten om digitala tjänster*].

6. Denna förordning ska inte tillämpas på AI-system, inbegripet deras utdata, som specifikt utvecklas och tas i bruk enbart i vetenskapligt forsknings- och utvecklingssyfte.

7. Denna förordning ska inte tillämpas på forsknings- och utvecklingsverksamhet som rör AI-system.

8. Denna förordning ska inte tillämpas på skyldigheter för användare som är fysiska personer som använder AI-system inom ramen för en rent personlig icke-yrkesmässig verksamhet, med undantag för artikel 52.

---

[31] 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).

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

(1) *system med artificiell intelligens* (*AI-system*): ett system som utformats för att arbeta med inslag av autonomi och som, på grundval av data och indata som tillhandahållits av maskin och/eller människa, drar slutsatser om hur en viss uppsättning mål ska uppnås med användning av metoder för maskininlärning och/eller logik- och kunskapsbaserade metoder och producerar systemgenererade utdata såsom innehåll, (system för generativ AI) förutsägelser, rekommendationer eller beslut som påverkar de miljöer som AI-systemet samverkar med.

1a. *ett AI-systems livscykel*: ett AI-systems varaktighet, från design till tillbakadragande. Utan att det påverkar marknadskontrollmyndigheternas befogenheter kan ett sådant tillbakadragande ske när som helst under fasen av övervakning efter utsläppande på marknaden efter beslut av leverantören och det ska innebära att systemet inte får användas längre. Ett AI-systems livscykel ska även avslutas genom en väsentlig ändring av AI-systemet som görs av leverantören eller någon annan fysisk eller juridisk person, i vilket fall det väsentligt ändrade AI-systemet ska anses vara ett nytt AI-system.

1b. *AI-system för allmänna ändamål*: ett AI-system som – oavsett på vilket sätt det släpps ut på marknaden eller tas i bruk, inbegripet i form av programvara med öppen källkod – av leverantören är avsett att utföra allmänt tillämpliga funktioner såsom bild- och taligenkänning, ljud- och videoupptagning, mönsterdetektering, frågebesvarande, översättning och andra. Ett AI-system för allmänna ändamål kan användas i ett flertal sammanhang och integreras i ett flertal andra AI-system.

(2) *leverantör*: en fysisk eller juridisk person, en offentlig myndighet, en byrå eller ett annat organ som utvecklar eller låter utveckla ett AI-system och släpper ut det systemet på marknaden eller tar det i bruk i eget namn eller under eget varumärke, antingen mot betalning eller kostnadsfritt.

(3) [utgår]

3a. *små och medelstora företag*: företag enligt definitionen i artikel 2.1 i bilagan till kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag.

4. *användare*: varje fysisk eller juridisk person, inbegripet en offentlig myndighet, en byrå eller ett annat organ, under vars överinseende systemet används.

5. *ombud*: en fysisk eller juridisk person som är fysiskt närvarande eller etablerad i unionen och som har fått och godtagit skriftlig fullmakt från en leverantör av ett AI-system att för dennes räkning fullgöra respektive genomföra de skyldigheter och förfaranden som fastställs i denna förordning.

5a. *produkttillverkare*: en tillverkare i den mening som avses i unionens harmoniseringslagstiftning enligt förteckningen i bilaga II.

6. *importör*: en fysisk eller juridisk person som är fysiskt närvarande eller 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 utanför unionen.

7. *distributör*: en fysisk eller juridisk person i leveranskedjan, utöver tillverkaren eller importören, som tillhandahåller ett AI-system på unionsmarknaden.

8. *operatör*: leverantören, produkttillverkaren, användaren, ombudet, importören eller distributören.

9. *utsläppande på marknaden*: den första gången ett AI-system tillhandahålls på unionsmarknaden.

10. *tillhandahållande på marknaden*: varje leverans av ett AI-system för distribution eller användning på unionsmarknaden i samband med kommersiell verksamhet, mot betalning eller kostnadsfritt.

11. *ibruktagande*: leverans av ett AI-system för första användning direkt till användaren 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 sammanhanget 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.

14. *säkerhetskomponent i en produkt eller ett system*: 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 användaren 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 ett AI-system som tillhandahållits för användare.

17. *tillbakadragande av ett AI-system*: åtgärd för 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. *bedömning av överensstämmelse*: processen där det kontrolleras om kraven i avdelning III kapitel 2 i denna förordning avseende ett AI-system med hög risk har uppfyllts.

20. *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.

21. *organ för bedömning av överensstämmelse*: organ som utför tredjepartsbedömning av överensstämmelse, inbegripet testning, certifiering och kontroll.

22. *anmält organ*: organ för bedömning av överensstämmelse som utsetts i enlighet med denna förordning och annan relevant unionslagstiftning om harmonisering.

23. *väsentlig ändring*: en ändring av AI-systemet som gjorts efter dess utsläppande på marknaden eller ibruktagande och som påverkar AI-systemets uppfyllelse av kraven i avdelning III kapitel 2 i denna förordning, eller en ändring av det avsedda ändamål för vilket AI-systemet har bedömts. 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.

24. *CE-märkning om överensstämmelse* (*CE-märkning*): märkning genom vilken en leverantör anger att ett AI-system överensstämmer med kraven i avdelning III kapitel 2 eller artikel 4b i denna förordning och annan tillämplig unionsrättsakt som harmoniserar villkoren för saluföring av produkter (*unionens harmoniseringslagstiftning*) och som föreskriver sådan märkning.

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 europeisk 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 denna förordning.

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, bland annat, för att förhindra överanpassning. Valideringsdatasetet kan vara ett separat dataset eller en del av träningsdatasetet, antingen som en fast eller variabel uppdelning.

31. *testdata*: data som används för att tillhandahålla en oberoende utvärdering av det tränade och validerade AI-systemet för att bekräfta systemets förväntade prestanda innan det släpps ut på marknaden eller tas i bruk.

32. *indata*: data som lämnas till eller förvärvas direkt av ett AI-system och som utgör den grund på vilken systemet producerar utdata.

33. *biometriska uppgifter*: personuppgifter som erhållits genom särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken, såsom ansiktsbilder eller fingeravtrycksuppgifter.

34. *system för känsloigenkänning*: ett AI-system vars syfte är att identifiera eller uttyda fysiska personers psykologiska tillstånd, känslor eller avsikter på grundval av deras biometriska uppgifter.

35. *system för biometrisk kategorisering*: ett AI-system vars syfte är att hänföra fysiska personer till särskilda kategorier på grundval av deras biometriska uppgifter.

36. *system för biometrisk fjärridentifiering*: ett AI-system vars syfte är att identifiera fysiska personer, vanligtvis på distans, utan deras aktiva medverkan, genom jämförelse av en persons biometriska uppgifter med de biometriska uppgifterna i ett referenscentrallager för databaser.

37. *system för biometrisk fjärridentifiering i realtid*: ett system för biometrisk fjärridentifiering där insamling av biometriska uppgifter, jämförelse och identifiering sker omedelbart eller nästan omedelbart.

38. [utgår]

39. *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 har fastställts på förhand och oberoende av eventuella kapacitetsbegränsningar.

40. *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.

41. *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.

42. [utgår]

43. *nationell behörig myndighet*: någon av följande: den anmälande myndigheten och marknadskontrollmyndigheten. När det gäller AI-system som tas i bruk eller används av unionens institutioner, byråer, kontor och organ ska Europeiska datatillsynsmannen fullgöra det ansvar som i medlemsstaterna anförtros den nationella behöriga myndigheten, och i relevanta fall ska alla hänvisningar till nationella behöriga myndigheter eller marknadskontrollmyndigheter i denna förordning förstås som hänvisningar till Europeiska datatillsynsmannen.

44. *allvarlig incident*: en incident eller ett fel i ett AI-system som direkt eller indirekt orsakar något av följande:

a) Dödsfall eller allvarlig skada för en persons hälsa.

b) En allvarlig och oåterkallelig störning av förvaltningen och driften av kritisk infrastruktur.

c) Åsidosättande av skyldigheterna att skydda de grundläggande rättigheterna enligt unionsrätten.

d) Allvarlig skada för egendom eller för miljön.

45. *kritisk infrastruktur*: en tillgång, ett system eller en del därav som krävs för att tillhandahålla en tjänst som är nödvändig för att upprätthålla centrala samhällsfunktioner eller central ekonomisk verksamhet i den mening som avses i artikel 2.4 och 2.5 i direktiv .../... om kritiska entiteters motståndskraft.

46. *personuppgifter*: uppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.

47. *icke-personuppgifter*: andra uppgifter än personuppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.

48. *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; testning under verkliga förhållanden 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 53 eller artikel 54a är uppfyllda.

49. *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.

50. *försöksperson*: vid testning under verkliga förhållanden en fysisk person som deltar i testning under verkliga förhållanden.

51. *informerat samtycke*: en försökspersons fria och frivilliga 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; om försökspersonen är underårig eller inte är beslutskompetent, ska tillståndet eller samtycket lämnas av försökspersonens lagligen utsedda ställföreträdare.

52. *regulatorisk sandlåda för AI*: en konkret ram som inrättats av en nationell 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 plan för en begränsad tid under lagstadgad tillsyn.

Artikel 4

Genomförandeakter

För att säkerställa enhetliga villkor för genomförandet av denna förordning när det gäller metoder för maskininlärning och logik- och kunskapsbaserade metoder som avses i artikel 3.1 får kommissionen anta genomförandeakter för att specificera de tekniska delarna av dessa metoder, med beaktande av marknadsutvecklingen och den tekniska utvecklingen. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 74.2.

AVDELNING IA

AI-SYSTEM FÖR ALLMÄNNA ÄNDAMÅL

Artikel 4a

Förenlighet mellan AI-system för allmänna ändamål och denna förordning

1. Utan att det påverkar tillämpningen av artiklarna 5, 52, 53 och 69 i denna förordning ska AI-system för allmänna ändamål endast uppfylla de krav och skyldigheter som anges i artikel 4b.

2. Sådana krav och skyldigheter ska gälla oavsett om AI-systemet för allmänna ändamål släpps ut på marknaden eller tas i bruk som en förtränad modell och om ytterligare finjustering av modellen ska utföras av användaren av AI-systemet för allmänna ändamål.

Artikel 4b

Krav för AI-system för allmänna ändamål och skyldigheter för leverantörer av sådana system

1. AI-system för allmänna ändamål som kan användas som AI-system med hög risk eller som komponenter i AI-system med hög risk i den mening som avses i artikel 6 ska uppfylla de krav som fastställs i avdelning III kapitel 2 i denna förordning från och med tillämpningsdagen för de genomförandeakter som antas av kommissionen i enlighet med det granskningsförfarande som avses i artikel 74.2 senast 18 månader efter denna förordnings ikraftträdande. Dessa genomförandeakter ska specificera och anpassa tillämpningen av de krav som fastställs i avdelning III kapitel 2 på AI-system för allmänna ändamål mot bakgrund av deras egenskaper, tekniska genomförbarhet, särdrag i AI-värdekedjan samt marknadsutvecklingen och den tekniska utvecklingen. Vid uppfyllandet av dessa krav ska den allmänt erkända bästa tekniken beaktas.

2. Leverantörer av AI-system för allmänna ändamål som avses i punkt 1 ska från och med tillämpningsdagen för de genomförandeakter som avses i punkt 1 fullgöra de skyldigheter som anges i artiklarna 16aa, 16e, 16f, 16g, 16i, 16j, 25, 48 och 61.

3. För att fullgöra de skyldigheter som anges i artikel 16e ska leverantörerna följa det förfarande för bedömning av överensstämmelse som grundar sig på intern kontroll enligt punkterna 3 och 4 i bilaga VI.

4. Leverantörer av sådana system ska också hålla den tekniska dokumentation som avses i artikel 11 tillgänglig för de nationella behöriga myndigheterna under en period som löper ut tio år efter det att AI-systemet för allmänna ändamål har släppts ut på unionsmarknaden eller tagits i bruk i unionen.

5. Leverantörer av AI-system för allmänna ändamål ska samarbeta med och tillhandahålla nödvändig information till andra leverantörer som avser att ta i bruk eller släppa ut sådana system på unionsmarknaden som AI-system med hög risk eller som komponenter i AI-system med hög risk, i syfte att göra det möjligt för de senare att fullgöra sina skyldigheter enligt denna förordning. Vid sådant samarbete mellan leverantörer ska, när så är lämpligt, immateriella rättigheter samt konfidentiell affärsinformation eller företagshemligheter bevaras i enlighet med artikel 70. För att säkerställa enhetliga villkor för genomförandet av denna förordning vad gäller den information som ska delas av leverantörer av AI-system för allmänna ändamål får kommissionen anta genomförandeakter i enlighet med det granskningsförfarande som avses i artikel 74.2.

6. För att uppfylla de krav och fullgöra de skyldigheter som avses i punkterna 1, 2 och 3 ska

– alla hänvisningar till det avsedda ändamålet förstås som en hänvisning till eventuell användning av AI-system för allmänna ändamål som AI-system med hög risk eller som komponenter i AI-system med hög risk i den mening som avses i artikel 6,

– varje hänvisning till kraven för AI-system med hög risk i avdelning III kapitel II förstås som en hänvisning endast till de krav som anges i den här artikeln.

Artikel 4c

Undantag från artikel 4b

1. Artikel 4b ska inte tillämpas om leverantören uttryckligen har uteslutit all användning med hög risk i bruksanvisningen eller i den information som åtföljer AI-systemet för allmänna ändamål.

2. Ett sådant undantag ska göras i god tro och inte anses vara motiverat om leverantören har tillräckliga skäl att anse att systemet kan komma att användas felaktigt.

3. När leverantören upptäcker eller informeras om felaktig användning på marknaden ska denna vidta alla nödvändiga och proportionella åtgärder för att förhindra sådan ytterligare felaktig användning, särskilt med beaktande av den felaktiga användningens omfattning och av hur allvarliga de därmed förknippade riskerna är.

AVDELNING II

FÖRBJUDNA TILLÄMPNINGAR AV ARTIFICIELL INTELLIGENS

Artikel 5

1. Följande AI-tillämpningar ska vara förbjudna:

a) Utsläppande på marknaden, ibruktagande eller användning av ett AI-system som använder subliminala tekniker som människor inte är medvetna om med målet eller verkan att väsentligt snedvrida en persons beteende på ett sätt som orsakar eller rimligt sannolikt kommer att orsaka fysisk eller psykisk skada för den personen eller en annan person.

b) Utsläppande på marknaden, ibruktagande eller användning av ett AI-system som utnyttjar någon sårbarhet hos 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 en person som tillhör den gruppen på ett sätt som orsakar eller rimligt sannolikt kommer att orsaka fysisk eller psykisk 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 under en viss tidsperiod på grundval av deras sociala beteende eller kända 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 grupper av fysiska 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 fysiska personer som är omotiverad eller oproportionerlig i förhållande till personernas sociala beteende eller till hur allvarligt beteendet är.

d) Användning av system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser av brottsbekämpande myndigheter eller på deras vägnar, såvida inte och endast i den mån sådan användning är absolut nödvändig för något av följande syften:

i) Målinriktad sökning efter specifika potentiella brottsoffer.

ii) Förhindrande av ett specifikt och betydande hot mot den kritiska infrastrukturen, hälsa, fysiska personers liv eller fysiska säkerhet eller förebyggande av terroristattacker.

iii) lokalisering eller identifiering av en fysisk person i syfte att genomföra en brottsutredning, lagföring eller ett verkställande av en straffrättslig påföljd för brott som avses i artikel 2.2 i rådets rambeslut 2002/584/JHA[32] och som i den berörda medlemsstaten kan bestraffas med fängelse eller annan frihetsberövande åtgärd under en maximal tidsperiod på minst tre år, eller andra specifika brott som i den berörda medlemsstaten kan leda till fängelse eller annan frihetsberövande åtgärd under en maximal tidsperiod på minst fem år enligt den medlemsstatens lagstiftning.

2. Vid användning av system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpningsändamål för något av de syften som avses i punkt 1 d ska följande faktorer beaktas:

a) Arten av den situation som ger upphov till den eventuella användningen, särskilt vad gäller hur allvarlig och omfattande skadan blir, och sannolikheten för att den uppstår om systemet inte används.

[32] 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).

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 system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpningsändamål för något av de syften som avses i punkt 1 d vara förenlig med nödvändiga och proportionella skyddsåtgärder och villkor avseende användningen, särskilt vad gäller tidsmässiga och geografiska begränsningar samt personbegränsningar.

3. När det gäller punkterna 1 d 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 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 4. I vederbörligen motiverade brådskande situationer får dock användningen av systemet påbörjas utan tillstånd, förutsatt att ett sådant tillstånd ska begäras utan onödigt dröjsmål under användningen av AI-systemet, och om ett sådant tillstånd avslås ska AI-systemets användning upphöra med omedelbar verkan.

Den behöriga rättsliga eller administrativa myndigheten 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 aktuella systemet för biometrisk fjärridentifiering i realtid är nödvändig och proportionerlig för att uppnå ett av de syften som anges i punkt 1 d, i enlighet med vad som anges i begäran. Vid beslut om begäran ska den behöriga rättsliga eller administrativa myndigheten beakta de faktorer som avses i punkt 2.

4. 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 d, 2 och 3. Den medlemsstaten ska i sin nationella lagstiftning fastställa de nödvändiga detaljerade reglerna för begäran om, utfärdande av och användning av, samt utövande av 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 d, inbegripet vilka av de brott som avses i led iii i punkten, de behöriga myndigheterna kan få tillstånd att använda dessa system för brottsbekämpningsändamål.

AVDELNING III

AI-SYSTEM MED HÖG RISK

KAPITEL 1

KLASSIFICERING AV AI-SYSTEM SOM HÖGRISKSYSTEM

Artikel 6

Klassificeringsregler för AI-system med hög risk

1. Ett AI-system som i sig är en produkt som omfattas av unionens harmoniseringslagstiftning enligt förteckningen i bilaga II ska betraktas som ett högrisksystem om det krävs en tredjepartsbedömning av överensstämmelse för att produkten ska kunna släppas ut på marknaden eller tas i bruk i enlighet med ovannämnda lagstiftning.

2. Ett AI-system som är avsett att användas som en säkerhetskomponent i en produkt som omfattas av den lagstiftning som avses i punkt 1 ska betraktas som högrisksystem om det krävs en tredjepartsbedömning av överensstämmelse för att produkten ska kunna släppas ut på marknaden eller tas i bruk i enlighet med ovannämnda lagstiftning. Denna bestämmelse ska tillämpas oavsett om AI-systemet släpps ut på marknaden eller tas i bruk fristående från produkten.

3. AI-system som avses i bilaga III ska betraktas som system med hög risk, såvida inte systemets utdata endast är helt accessoriska med avseende på den relevanta åtgärd som ska vidtas eller det relevanta beslut som ska fattas och därför sannolikt inte kommer att leda till någon betydande risk för hälsa, säkerhet eller grundläggande rättigheter.

För att säkerställa enhetliga villkor för genomförandet av denna förordning ska kommissionen senast ett år efter denna förordnings ikraftträdande anta genomförandeakter för att specificera under vilka omständigheter utdata från AI-system som avses i bilaga III endast skulle vara rent accessoriska med avseende på den relevanta åtgärd som ska vidtas eller det relevanta beslut som ska fattas. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 74.2.

Artikel 7

Ändringar av bilaga III

1. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 73 med avseende på att ändra förteckningen i bilaga III genom att lägga till 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 punkterna 1–8 i bilaga III.

   b) AI-systemen utgör en risk för skada på hälsa och säkerhet, eller en risk för negativ inverkan på grundläggande rättigheter, med beaktande av skadans allvarlighetsgrad och sannolikheten för att den ska uppstå, som 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 tillämpningen av punkt 1 ska kommissionen beakta följande kriterier när den bedömer om ett AI-system utgör en risk för skada på hälsa och säkerhet eller en risk för negativ inverkan på grundläggande rättigheter som är likvärdig med eller större än den risk för skada som skapas av de AI-system med hög risk som redan nämns i bilaga III:

a) Det avsedda ändamålet med AI-systemet.

b) I vilken utsträckning ett AI-system har använts eller sannolikt kommer att användas.

c) I vilken utsträckning användningen av ett AI-system redan har orsakat skada på hälsa och säkerhet eller negativ inverkan på de grundläggande rättigheterna eller har gett upphov till betydande farhågor när det gäller uppkomsten av sådan skada eller negativ inverkan, såsom framgår av rapporter eller dokumenterade anklagelser som lämnats till nationella behöriga myndigheter.

d) Den potentiella omfattningen av sådan skada eller sådan negativ inverkan, särskilt i fråga om intensitet och förmåga att påverka en stor mängd personer.

e) 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.

f) I vilken utsträckning potentiellt skadade eller negativt påverkade personer befinner sig i ett utsatt läge i förhållande till användaren av ett AI-system, särskilt på grund av en obalans i fråga om makt, kunskap, ekonomiska eller sociala omständigheter eller ålder.

g) I vilken utsträckning det resultat som produceras med ett AI-system inte är lätt att upphäva, varvid resultat som påverkar människors hälsa eller säkerhet inte ska anses vara lätta att upphäva.

h) I vilken utsträckning befintlig unionslagstiftning 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.

i) Omfattningen av och sannolikheten för fördelar med AI-användningen för enskilda personer, grupper eller samhället som helhet.

3. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 73 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 eller de berörda AI-systemen medför inte länger 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.

KAPITEL 2

KRAV FÖR AI-SYSTEM MED HÖG RISK

Artikel 8

Uppfyllelse av kraven

1. AI-system med hög risk ska uppfylla de krav som fastställs i detta kapitel med beaktande av den allmänt erkända bästa tekniken.

2. Det avsedda ändamålet med AI-systemet med hög risk och det riskhanteringssystem som avses i artikel 9 ska beaktas när uppfyllelsen av dessa krav säkerställs.

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 uppdatering. Det ska innehålla följande steg:

   a) Identifiering och analys av de kända och förutsebara risker som med störst sannolikhet kommer att uppstå för hälsa, säkerhet och grundläggande rättigheter med tanke på det avsedda ändamålet med AI-systemet med hög risk.

   b) [utgår]

   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 61.

   d) Antagande av lämpliga riskhanteringsåtgärder i enlighet med bestämmelserna i följande punkter.

   De risker som avses i denna punkt 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.

3. 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 kapitel 2, i syfte att minimera riskerna mer effektivt och samtidigt uppnå en lämplig balans i genomförandet av åtgärderna för att uppfylla dessa krav.

4. De riskhanteringsåtgärder som avses i punkt 2 d ska vara sådana att eventuella 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 möjligt genom lämplig konstruktion och utveckling av AI-systemet med hög risk.

b) När det är lämpligt, genomförande av lämpliga åtgärder för att begränsa och bemästra risker som inte kan elimineras.

c) Tillhandahållande av tillräcklig information enligt artikel 13, särskilt när det gäller de risker som avses i punkt 2 b i denna artikel och, i förekommande fall, utbildning för användare.

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 användaren förväntas ha och den miljö där systemet är avsett att användas.

5. AI-system med hög risk ska testas för att säkerställa att de fungerar på ett sätt som är förenligt med deras avsedda ändamål och att de uppfyller kraven i detta kapitel.

6. Testningsförfarandena får omfatta testning under verkliga förhållanden i enlighet med artikel 54a.

7. 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.

8. Det riskhanteringssystem som beskrivs i punkterna 1–7 ska ta särskild hänsyn till huruvida personer som är yngre än 18 år sannolikt kommer att ha tillgång till eller påverkas av AI-systemet med hög risk.

9. För leverantörer av AI-system med hög risk som omfattas av krav avseende interna riskhanteringsprocesser enligt relevant sektorsspecifik unionslagstiftning får de aspekter som beskrivs i punkterna 1–8 ingå i 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 modeller med data ska utvecklas på grundval av tränings-, validerings- och testningsdataset som uppfyller de kvalitetskriterier som avses i punkterna 2–5.

2. Tränings-, validerings- och testningsdataset ska omfattas av ändamålsenliga metoder för dataförvaltning och datahantering. Dessa metoder ska särskilt avse

   a) relevanta konstruktionsval,

   b) datainsamlingsprocesser,

   c) relevanta åtgärder för datapreparering, såsom annotation, märkning, uppstädning, förädling och aggregering,

d) formulering av relevanta antaganden, särskilt när det gäller den information som berörda data förväntas beskriva och representera,

e) en förhandsbedömning av tillgängligheten, mängden och lämpligheten avseende de dataset som behövs,

f) undersökning med avseende på eventuella snedvridningar som kan påverka fysiska personers hälsa och säkerhet eller leda till diskriminering som är förbjuden enligt unionsrätten,

g) identifiering av alla eventuella dataluckor eller brister, och hur dessa luckor och brister kan åtgärdas.

3. Tränings-, validerings- och testningsdataset ska vara relevanta, och representativa, och så långt som möjligt felfria och fullständiga. De ska ha lämpliga statistiska egenskaper, däribland, i förekommande fall, vad gäller de personer eller grupper av personer som omfattas av den avsedda användningen av AI-systemet med hög risk. Dessa egenskaper hos dessa dataset kan uppfyllas på nivån för enskilda dataset eller en kombination av dessa.

4. Tränings-, validerings- och testningsdataset 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, 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 övervakning, upptäckt och korrigering av snedvridning i samband med AI-systemen med hög risk, får leverantörer av sådana system behandla särskilda 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, med förbehåll för lämpliga skyddsåtgärder för fysiska personers grundläggande rättigheter och friheter, inbegripet tekniska begränsningar för vidareutnyttjande samt användning av säkerhetsåtgärder och integritetsbevarande åtgärder på aktuell teknisk nivå, såsom pseudonymisering, eller kryptering där anonymisering avsevärt kan påverka det eftersträvade ändamålet.

6. För utvecklingen av AI-system med hög risk som inte använder teknik som inbegriper träning av modeller ska punkterna 2–5 tillämpas endast på testningsdataset.

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 uppfyller kraven i detta kapitel, och så att nationella behöriga myndigheter och anmälda organ får all 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 eller, när det gäller små och medelstora företag, inbegripet nystartade företag, all likvärdig dokumentation som uppfyller samma mål, såvida inte den behöriga myndigheten bedömer den vara olämplig.

2. Om ett AI-system med hög risk som är kopplat till en produkt, som omfattas av de rättsakter som förtecknas i avsnitt A i bilaga II, släpps ut på marknaden eller tas i bruk ska en enda teknisk dokumentation upprättas som innehåller all den information som anges i bilaga IV samt den information som krävs enligt dessa rättsakter.

3. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 73 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 om systemet uppfyller kraven i detta kapitel.

Artikel 12

Arkivering

1. AI-system med hög risk ska tekniskt möjliggöra automatisk registrering av händelser (loggar) under hela systemets livscykel.

2. För att säkerställa en spårbarhetsnivå för AI-systemets funktion som är lämplig för systemets avsedda ändamål ska loggningskapaciteten möjliggöra registrering av händelser som är relevanta för

   i) identifiering av situationer som kan resultera i att AI-systemet utgör en risk i den mening som avses i artikel 65.1 eller i en väsentlig ändring,

   ii) underlättande av den övervakning efter utsläppande på marknaden som avses i artikel 61 och

   iii) övervakning av driften av AI-system med hög risk som avses i artikel 29.4.

4. 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 användare

1. AI-system med hög risk ska utformas och utvecklas på ett sådant sätt att driften av dem är tillräckligt transparent i syfte att uppnå uppfyllelse av användarens och leverantörens relevanta skyldigheter enligt kapitel 3 i denna avdelning och göra det möjligt för användare att förstå och använda systemet på lämpligt sätt.

2. AI-system med hög risk ska åtföljas av en bruksanvisning i ett lämpligt digitalt format eller på annat sätt som inbegriper kortfattad, fullständig, korrekt och tydlig information som är relevant, tillgänglig och begriplig för användare.

3. I den information som avses i punkt 2 ska följande specificeras:

   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, inklusive den specifika geografiska, beteendemässiga eller funktionella miljö inom vilken AI-systemet med hög risk är avsett att användas,

      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 och som kan leda till de risker för hälsa och säkerhet eller grundläggande rättigheter som avses i artikel 9.2,

iv) i lämpliga fall, dess beteende vad gäller specifika personer eller grupper av personer som omfattas av den avsedda användningen av systemet,

v) i tillämpliga fall, specifikationer för indata, eller all annan relevant information i fråga om de tränings-, valideringss- och testningsdataset som används, med beaktande av AI-systemets avsedda ändamål.

vi) i lämpliga fall, en beskrivning av systemets förväntade utdata.

c) Eventuella ändringar av AI-systemet med hög risk och dess prestanda som leverantören i förväg 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 användarnas tolkning av AI-systemens utdata.

e) De data- och maskinvaruresurser som krävs, den förväntade livslängden för AI-systemet med hög risk och alla nödvändiga underhålls- och omsorgsåtgärder, inbegripet deras frekvens, för att säkerställa att AI-systemet fungerar korrekt, även när det gäller programvaruuppdateringar.

f) En beskrivning av de mekanismer som ingår i AI-systemet och som gör det möjligt för användarna att korrekt samla in, lagra och tolka loggarna, om detta är relevant.

Artikel 14

Mänsklig tillsyn

1. AI-system med hög risk ska utformas och utvecklas på ett sådant sätt, inbegripet med lämpliga verktyg för användargränssnitt mellan människa och maskin, 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 kapitel.

3. Mänsklig tillsyn ska säkerställas genom antingen en eller samtliga 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 användaren.

4. Vid genomförandet av punkterna 1–3 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 omständigheterna

   a) förstå kapaciteten och begränsningarna hos AI-systemet med hög risk och på vederbörligt sätt kunna övervaka dess drift.

   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”),

   c) korrekt kunna tolka utdata från AI-systemet med hög risk, särskilt 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 ”stoppknapp” eller ett liknande förfarande,

5. För AI-system med hög risk som avses i punkt 1 a i bilaga III ska de åtgärder som avses i punkt 3 dessutom vara sådana att de säkerställer att ingen åtgärd och inget beslut vidtas respektive fattas av användaren på grundval av den identifiering som systemet resulterar i, såvida inte detta har kontrollerats och bekräftats separat av minst två fysiska personer. Kravet på en separat kontroll av minst två fysiska personer ska inte tillämpas på AI-system med hög risk som används för brottsbekämpning, migration, gränskontroll eller asyl, i fall där unionsrätten eller nationell rätt anser att tillämpningen av detta krav är oproportionell.

Artikel 15

Noggrannhet, robusthet och cybersäkerhet

1. AI-system med hög risk ska utformas och utvecklas på ett sådant sätt att de, mot bakgrund av sitt avsedda ändamål, uppnår en lämplig nivå avseende noggrannhet, robusthet och cybersäkerhet och ger bra resultat i dessa avseenden under hela sin livscykel.

2. Noggrannhetsnivåerna och relevanta noggrannhetsmått för AI-system med hög risk ska anges i de medföljande bruksanvisningarna.

3. AI-system med hög risk ska vara resilienta 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.

   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 hanteras på vederbörligt sätt med lämpliga kompenserande åtgärder.

4. AI-system med hög risk ska vara resilienta mot försök av obehöriga tredje parter att ändra sin användning 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 och bekämpa attacker som försöker manipulera träningsdatasetet (”dataförgiftning”), indata som är utformade för att få modellen att göra ett misstag (”antagonistiska exempel”) eller modellfel.

KAPITEL 3

SKYLDIGHETER FÖR LEVERANTÖRER OCH ANVÄNDARE 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 kapitel 2 i denna avdelning,

aa) ange sitt namn, sitt registrerade firmanamn eller sitt registrerade varumärke, en kontaktadress 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,

b) ha ett kvalitetsstyrningssystem som uppfyller kraven i artikel 17,

c) förvara den dokumentation som avses i artikel 18,

d) spara de loggar som genereras automatiskt av deras AI-system med hög risk enligt artikel 20, när loggarna står under deras kontroll,

e) 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,

f) fullgöra de registreringsskyldigheter som avses i artikel 51.1,

g) vidta nödvändiga korrigerande åtgärder enligt artikel 21 om AI-systemet med hög risk inte uppfyller kraven i kapitel 2 i denna avdelning,

h) informera den berörda nationella behöriga myndigheten i de medlemsstater där de har tillhandahållit eller tagit AI-systemet i bruk och, i tillämpliga fall, det anmälda organet, om den bristande överensstämmelsen och om eventuella korrigerande åtgärder som vidtagits,

i) anbringa CE-märkningen på sina AI-system med hög risk för att påvisa överensstämmelse med denna förordning i enlighet med artikel 49,

j) på begäran av en nationell behörig myndighet visa att AI-systemet med hög risk uppfyller kraven i kapitel 2 i denna avdelning.

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, de medel som ska användas för att säkerställa att AI-systemet med hög risk uppfyller kraven i kapitel 2 i denna avdelning.

f) System och förfaranden för datahantering, inbegripet datainsamling, 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 61.

i) Förfaranden som berör rapportering av en allvarlig incident i enlighet med artikel 62.

j) Hantering av kommunikation med nationella behöriga myndigheter, behöriga myndigheter, inbegripet sektorsmyndigheter, 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 alla aspekter som anges i denna punkt.

2. Genomförandet av aspekter som avses i punkt 1 ska stå i proportion till storleken på leverantörens organisation.

2a. För leverantörer av AI-system med hög risk som omfattas av skyldigheter avseende kvalitetsstyrningsprocesser enligt relevant sektorsspecifik unionslagstiftning får de aspekter som beskrivs i punkt 1 ingå i de kvalitetsstyrningssystem som fastställs i enlighet med den lagstiftningen.

3. För leverantörer som är finansiella institut som omfattas av krav avseende interna styrelseformer, arrangemang eller processer enligt unionslagstiftningen om finansiella tjänster ska skyldigheten att införa ett kvalitetsstyrningssystem, med undantag för punkt 1 g, h och i, anses vara uppfylld genom att reglerna om interna styrelseformer, arrangemang eller processer efterlevs enligt relevant unionslagstiftning om finansiella tjänster. I detta sammanhang ska alla harmoniserade standarder som avses i artikel 40 i denna förordning beaktas.

Artikel 18

Bevarande av dokumentation

1. Leverantören ska under en period på 10 år efter det att AI-systemet 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 48.

1a. 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.

2. Leverantörer som är finansiella institut som omfattas av krav avseende sin interna styrelseformer, arrangemang eller processer enligt unionslagstiftningen om finansiella tjänster ska bevara den tekniska dokumentationen som en del av den dokumentation som ska bevaras enligt relevant unionslagstiftning om finansiella tjänster.

Artikel 19

Bedömning av överensstämmelse

1. Leverantörer av AI-system med hög risk ska säkerställa att deras system genomgår det relevanta förfarandet för bedömning av överensstämmelse i enlighet med artikel 43 innan de släpps ut på marknaden eller tas i bruk. Om AI-systemens överensstämmelse med kraven i kapitel 2 i denna avdelning har påvisats efter denna bedömning av överensstämmelse ska leverantörerna upprätta en EU-försäkran om överensstämmelse i enlighet med artikel 48 och anbringa CE-märkningen om överensstämmelse i enlighet med artikel 49.

2. [utgår]

Artikel 20

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 genom ett avtal med användaren eller på annat sätt enligt lag. De ska spara dem 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 finansiella institut som omfattas av krav avseende sina interna styrelseformer, arrangemang eller processer enligt unionslagstiftningen 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 lagstiftning om finansiella tjänster.

Artikel 21

Korrigerande åtgärder

Tillverkare 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 utreda, i tillämpliga fall, orsakerna i samarbete med den rapporterande användaren och vidta de korrigerande åtgärder som krävs för att, beroende på vad som är lämpligt, få systemet att överensstämma med kraven, dra tillbaka det eller återkalla det. De ska underrätta distributörerna av det aktuella AI-systemet med hög risk och, i förekommande fall, ombudet och importörerna om detta.

Artikel 22

Informationsplikt

Om AI-systemet med hög risk utgör en risk i den mening som avses i artikel 65.1 och denna risk är känd för systemleverantören, ska den leverantören omedelbart informera de nationella behöriga myndigheterna i de medlemsstater där den har tillhandahållit systemet och, i tillämpliga fall, det anmälda organ som utfärdat ett intyg för AI-systemet med hög risk, särskilt om den bristande överensstämmelsen och om eventuella korrigerande åtgärder som vidtagits.

Artikel 23

Samarbete med behöriga myndigheter

Leverantörer av AI-system med hög risk ska på begäran av en nationell 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 kapitel 2 i denna avdelning, på ett språk som är lätt att förstå för den berörda medlemsstatens myndighet. På motiverad begäran av en nationell behörig myndighet ska leverantörer också ge den myndigheten tillgång till de loggar enligt artikel 12.1 som genereras automatiskt av AI-systemet med hög risk, i den mån sådana loggar står under deras kontroll genom ett avtal med användaren eller på annat sätt enligt lag.

Artikel 23a

Villkor för att andra personer ska omfattas av en leverantörs skyldigheter

1. Varje fysisk eller juridisk person ska vid tillämpningen av denna förordning anses vara en leverantör av ett nytt 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 ska fördelas på annat sätt.

b) [utgår]

c) De gör en väsentlig ändring av ett AI-system med hög risk som redan har släppts ut på marknaden eller tagits i bruk.

d) De ändrar det avsedda ändamålet för ett AI-system som inte har hög risk och som redan släppts ut på marknaden eller tagits i bruk, så att det ändrade systemet kommer att utgöra ett AI-system med hög risk.

e) De släpper ut på marknaden eller tar i bruk ett AI-system för allmänna ändamål som ett AI-system med hög risk eller som en komponent i ett AI-system med hög risk.

2. Om de omständigheter som avses i punkt 1 a eller c uppstår, ska den leverantör som ursprungligen släppte ut AI-systemet med hög risk på marknaden eller tog det i bruk inte längre anses vara en leverantör vid tillämpningen av denna förordning.

3. För AI-system med hög risk som är säkerhetskomponenter i produkter som omfattas av de rättsakter som förtecknas i bilaga II avsnitt A, ska tillverkaren av dessa produkter anses vara leverantören av AI-systemet med hög risk och omfattas av skyldigheter som avses i artikel 16 enligt något av följande scenarier:

i) AI-systemet med hög risk släpps ut på marknaden tillsammans med produkten under produkttillverkarens namn eller varumärke.

ii) AI-systemet med hög risk tas i bruk under produkttillverkarens namn eller varumärke efter det att produkten släppts ut på marknaden.

Artikel 24

[utgår]

Artikel 25

Ombud

1. Innan leverantörer etablerade utanför unionen tillhandahåller sina system på unionsmarknaden ska de genom skriftlig fullmakt utse ett ombud som är etablerat i unionen.

2. Ombudet ska utföra de uppgifter som anges i fullmakten från leverantören. Vid tillämpning av denna förordning ska fullmakten ge ombudet befogenhet att utföra endast följande uppgifter:

-a) Kontrollera att EU-försäkran om överensstämmelse och den tekniska dokumentationen har upprättats och att leverantören har utfört ett lämpligt förfarande för bedömning av överensstämmelse.

a) Under en period som löper ut tio år efter det att AI-systemet med hög risk har släppts ut på marknaden eller tagits i bruk hålla kontaktuppgifterna till den leverantör genom vilken ombudet har utsetts, 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 som avses i artikel 63.7.

b) På motiverad begäran ge en nationell behörig myndighet all information och dokumentation, inbegripet den som innehas i enlighet med led b, som är nödvändig för att visa att ett AI-system med hög risk överensstämmer med kraven i kapitel 2 i denna avdelning, 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 genom ett avtal med användaren eller på annat sätt enligt lag.

c) På motiverad begäran samarbeta med nationella behöriga myndigheter om eventuella åtgärder som dessa vidtar med avseende på AI-systemet med hög risk.

d) Fullgöra de registreringsskyldigheter som avses i artikel 51.1 och, om registreringen av systemet utförs av leverantören själv, kontrollera att den information som avses i punkterna 1–11 i bilaga VIII del II är korrekt.

Ombudet ska säga upp fullmakten om denne har tillräckliga skäl att anse 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 är etablerat samt, i tillämpliga fall, det berörda anmälda organet om uppsägningen av fullmakten och skälen till detta.

Ombudet ska vara juridiskt ansvarigt för AI-system med säkerhetsbrister på samma grunder som, och vara solidariskt ansvarig med, leverantören med avseende på dess potentiella ansvar enligt rådets direktiv 85/374/EEG.

Artikel 26

Importörers skyldigheter

1. Innan importörer av AI-system med hög risk släpper ut ett sådant system på marknaden ska de säkerställa att systemet i fråga överensstämmer med denna förordning genom att kontrollera att

a) det tillämpliga förfarandet för bedömning av överensstämmelse enligt artikel 43 har utförts av leverantören av det AI-systemet,

b) leverantören har upprättat den tekniska dokumentationen i enlighet med bilaga IV,

c) systemet är försett med erforderlig CE-märkning om överensstämmelse och åtföljs av EU-försäkran om överensstämmelse och bruksanvisning,

d) det ombud som avses i artikel 25 har fastställts av leverantören.

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 information ska den inte släppa ut det systemet på marknaden förrän AI-systemet har bringats i överensstämmelse med kraven. Om AI-systemet med hög risk utgör en risk i den mening som avses i artikel 65.1 ska importören informera leverantören av AI-systemet, ombuden och marknadskontrollmyndigheterna om detta.

3. Importörer ska ange sitt namn, sitt registrerade firmanamn eller sitt registrerade varumärke och en kontaktadress 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.

4. Importörer ska så länge de har ansvar för ett AI-system med hög risk säkerställa att, i förekommande fall, lagrings- eller transportförhållanden inte äventyrar dess överensstämmelse med kraven i kapitel 2 i denna avdelning.

4a. Importörer ska under en period som löper ut tio år efter det att AI-systemet 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.

5. 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 kapitel 2 i denna avdelning på ett språk som lätt kan förstås av den nationella behöriga myndigheten. I detta syfte ska de också säkerställa att den tekniska dokumentationen kan göras tillgänglig för dessa myndigheter.

5a. Importörerna ska samarbeta med de nationella behöriga myndigheterna om alla åtgärder som dessa myndigheter vidtar med avseende på ett AI-system för vilket de är importör.

Artikel 27

Distributörers skyldigheter

1. Innan distributörer tillhandahåller ett AI-system med hög risk på marknaden ska de kontrollera att AI-systemet med hög risk är försett med erforderlig CE-märkning om överensstämmelse, 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 skyldigheter enligt artikel 16 b respektive artikel 26.3.

2. Om en distributör anser eller har skäl att tro att ett AI-system med hög risk inte överensstämmer med kraven i kapitel 2 i denna avdelning, får distributören inte tillhandahålla AI-systemet med hög risk på marknaden förrän det systemet har bringats i överensstämmelse med dessa krav. Om systemet utgör en risk i den mening som avses i artikel 65.1 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 kapitel 2 i denna avdelning.

4. En distributör som anser eller har skäl att tro att ett AI-system med hög risk som denne har tillhandahållit på marknaden inte överensstämmer med kraven i kapitel 2 i denna avdelning 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 65.1 ska distributören omedelbart informera 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 AI-system med hög risk förse den myndigheten med all information och dokumentation om deras verksamhet enligt beskrivningen i punkterna 1–4.

5a. Distributörerna ska samarbeta med de nationella behöriga myndigheterna om alla åtgärder som dessa myndigheter vidtar med avseende på ett AI-system för vilket de är distributör.

Artikel 28

[utgår]

Artikel 29

Skyldigheter för användare av AI-system med hög risk

1. Användare av AI-system med hög risk ska använda sådana system i enlighet med de bruksanvisningar som åtföljer systemen, enligt punkterna 2 och 5 i denna artikel.

1a. Användarna ska tilldela fysiska personer som har den kompetens, utbildning och befogenhet som krävs uppgiften att utöva mänsklig tillsyn.

2. Skyldigheterna i punkterna 1 och 1a ska inte påverka andra användarskyldigheter enligt unionsrätten eller nationell rätt eller användarens handlingsutrymme när det gäller att organisera sina egna resurser och aktiviteter i syfte att genomföra de åtgärder för mänsklig tillsyn som leverantören anger.

3. Utan att det påverkar tillämpningen av punkt 1 ska användaren, i den mån användaren utövar kontroll över indata, säkerställa att indata är relevanta med tanke på det avsedda ändamålet med AI-systemet med hög risk.

4. Användarna ska genomföra mänsklig tillsyn och övervaka driften av AI-systemet med hög risk på grundval av bruksanvisningen. Om de har skäl att tro att användningen i enlighet med bruksanvisningen kan leda till att AI-systemet utgör en risk i den mening som avses i artikel 65.1 ska de informera leverantören eller distributören och tillfälligt stoppa användningen av systemet. De ska också informera leverantören eller distributören när de har identifierat en allvarlig incident och avbryta användningen av AI-systemet. Om användaren inte kan nå leverantören ska artikel 62 gälla i tillämpliga delar. Denna skyldighet ska inte omfatta känsliga operativa uppgifter om användare av AI-system som är brottsbekämpande myndigheter.

För användare som är finansiella institut som omfattas av krav avseende sina interna styrelseformer, arrangemang eller processer enligt unionslagstiftningen om finansiella tjänster ska övervakningsskyldigheten i första stycket anses vara uppfylld genom att reglerna om interna styrelseformer, arrangemang, processer och mekanismer enligt relevant unionslagstiftning om finansiella tjänster följs.

5. Användare av AI-system med hög risk ska spara de loggar enligt artikel 12.1 som genereras automatiskt av systemet i fråga, i den mån sådana loggar står under deras kontroll. De ska spara dem i minst sex månader, om inte annat föreskrivs i tillämplig unionsrätt eller nationell rätt, i synnerhet unionsrätten om skydd av personuppgifter.

Användare som är finansiella institut som omfattas av krav avseende sina interna styrelseformer, arrangemang eller processer enligt unionslagstiftningen om finansiella tjänster ska bevara loggar som en del av den dokumentation som ska bevaras enligt relevant unionslagstiftning om finansiella tjänster.

5a. Användare av AI-system med hög risk som är offentliga myndigheter, byråer eller organ, med undantag för brottsbekämpande myndigheter, gränskontrollmyndigheter, immigrationsmyndigheter eller asylmyndigheter, ska fullgöra de registreringsskyldigheter som avses i artikel 51. Om de finner att det system som de avser att använda inte har registrerats i den EU-databas som avses i artikel 60 ska de inte använda det systemet och ska informera leverantören eller distributören.

6. Användare av AI-system med hög risk ska använda den information som tillhandahålls enligt artikel 13 för att uppfylla sin skyldighet att genomföra en konsekvensbedömning avseende dataskydd enligt artikel 35 i förordning (EU) 2016/679 eller artikel 27 i direktiv (EU) 2016/680, i tillämpliga fall.

6a. Användarna ska samarbeta med de nationella behöriga myndigheterna om alla åtgärder som dessa myndigheter vidtar med avseende på ett AI-system för vilket de är användare.

KAPITEL 4

ANMÄLANDE MYNDIGHETER OCH ANMÄLDA ORGAN

Artikel 30

Anmälande myndigheter

1. Varje medlemsstat ska utse eller etablera minst en anmälande myndighet som ska ansvara 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.

2. Medlemsstaterna får bestämma att den bedömning och övervakning som avses i punkt 1 ska utföras av ett nationellt ackrediteringsorgan i den betydelse som anges i förordning (EG) nr 765/2008 och i enlighet därmed.

3. Anmälande myndigheter ska etableras, organiseras och drivas på ett sådant sätt att det inte uppstår någon intressekonflikt i förhållande till organen för bedömning av överensstämmelse och att objektiviteten och opartiskheten i deras verksamhet garanteras.

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 utfört bedömningen av dessa organ.

5. En anmälande myndighet får inte erbjuda eller utföra någon verksamhet som utförs av organ för bedömning av överensstämmelse, och den får inte heller erbjuda eller utföra konsulttjänster på kommersiell eller konkurrensmässig grund.

6. Anmälande myndigheter ska skydda erhållen konfidentiell information i enlighet med artikel 70.

7. Anmälande myndigheter ska förfoga över tillräckligt med personal med lämplig kompetens för att kunna utföra sina uppgifter.

8. [utgår]

Artikel 31

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 AI-system som organet för bedömning av överensstämmelse anser sig ha kompetens för samt ett ackrediteringsintyg, om det finns ett sådant, som utfärdats av ett nationellt ackrediteringsorgan och där det intygas att organet för bedömning av överensstämmelse uppfyller kraven i artikel 33. 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 hela det underlag som krävs för kontroll, erkännande och regelbunden tillsyn av att det uppfyller kraven i artikel 33. För anmälda organ som utsetts enligt annan unionslagstiftning om harmonisering får alla dokument och intyg kopplade till sådana 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 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 33 fortlöpande uppfylls.

Artikel 32

Anmälningsförfarande

1. De anmälande myndigheterna får endast anmäla de organ för bedömning av överensstämmelse som har uppfyllt kraven i artikel 33.

2. De anmälande myndigheterna ska anmäla dessa organ till kommissionen och de andra medlemsstaterna med hjälp av det elektroniska anmälningsverktyg som har utvecklats och förvaltas av kommissionen.

3. Den anmälan som avses i punkt 2 ska innehålla detaljerade uppgifter om bedömningarna av överensstämmelse, modulen eller modulerna för bedömning av överensstämmelse och de berörda AI-systemen samt ett relevant intyg om kompetens. Om en anmälan inte grundar sig på ett ackrediteringsintyg som avses i artikel 31.2 ska den anmälande myndigheten ge kommissionen och de andra medlemsstaterna 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 33.

4. Det berörda organet för bedömning av överensstämmelse får endast bedriva verksamhet som anmält organ om kommissionen eller de andra medlemsstaterna inte har rest invändningar inom två veckor efter en anmälan från en anmälande myndighet, i de fall ett ackrediteringsintyg enligt artikel 31.2 används, eller inom två månader efter en anmälan från den anmälande myndigheten, i de fall då styrkande handlingar som avses i artikel 31.3 används.

5. [utgår]

Artikel 33

Krav på anmälda organ

1. Ett anmält organ ska vara inrättat enligt nationell lagstiftning och vara en juridisk person.

2. Allmänna organ ska uppfylla de organisatoriska krav och krav på kvalitetsledning, resurser och processer som är nödvändiga för att organen ska kunna fullgöra sina uppgifter.

3. Det anmälda organets organisationsstruktur, ansvarsfördelning, rapporteringsvägar och driftsätt ska vara av den beskaffenheten att förtroende säkerställs för utförandet och resultaten av den bedömningsverksamhet som de anmälda organen utför.

4. Anmälda organ ska vara oberoende av den leverantör av AI-system med hög risk för vilken organet utför bedömning av överensstämmelse. Anmälda organ ska också vara oberoende av varje annan operatör som har ett ekonomiskt intresse i det AI-system med hög risk som bedöms samt av eventuella konkurrenter till leverantören.

5. 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.

6. Anmälda organ ska ha infört dokumenterade förfaranden som ska säkerställa att deras personal, kommittéer, dotterbolag, underleverantörer och andra associerade organ eller personal vid externa organ respekterar konfidentialiteten i enlighet med artikel 70 i fråga om den information som organen får kännedom om i samband med aktiviteter avseende 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.

7. Anmälda organ ska ha förfaranden för verksamhetsutövning som tar vederbörlig hänsyn till ett företags storlek, den sektor där det agerar, dess struktur samt det berörda AI-systemets komplexitet.

8. Anmälda organ ska teckna en lämplig ansvarsförsäkring för deras verksamhet avseende bedömning av överensstämmelse, såvida inte den medlemsstat i vilken de befinner sig tar på sig ansvaret i överensstämmelse med nationell rätt eller den medlemsstaten är direkt ansvarig för bedömningen av överensstämmelse.

9. Anmälda organ ska kunna utföra alla de uppgifter som de åläggs genom 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.

10. 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 den relevanta AI-tekniken, relevanta data och relevant databehandling och om de krav som fastställs i kapitel 2 i denna avdelning.

11. Anmälda organ ska delta i den samordningsverksamhet som avses i artikel 38. De ska också delta direkt eller vara företrädda i europeiska standardiseringsorganisationer, eller se till att de är medvetna om och har aktuella kunskaper om relevanta standarder.

12. [utgår]

Artikel 33a

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 33 gälla, på villkor att dessa krav omfattas av de tillämpliga harmoniserade standarderna.

Artikel 34

Dotterbolag och underleverantörer till anmälda organ

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 33 och informera den anmälande myndigheten om detta.

2. De anmälda organen ska ta det fulla ansvaret för underleverantörernas eller dotterbolagens uppgifter, oavsett var dessa är etablerade.

3. Verksamhet kan läggas ut på underentreprenad eller utföras av ett dotterbolag endast om leverantören samtycker därtill.

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 underleverantörsverksamheten.

Artikel 34a

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 avses i artikel 43.

2. Anmälda organ ska utföra sin verksamhet så att man samtidigt undviker onödiga bördor för leverantörer och, med vederbörligt beaktande av ett företags storlek, den sektor där detta agerar, dess struktur samt komplexiteten i det berörda AI-systemet med hög risk. Samtidigt ska det anmälda organet 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 göra tillgänglig och på begäran lämna över all relevant dokumentation, inbegripet leverantörens dokumentation, till den anmälande myndighet som hänvisas till i artikel 30, så att denna myndighet kan utföra sina uppgifter avseende bedömning, utseende, anmälan och övervakning och för att underlätta den bedömning som beskrivs i detta kapitel.

Artikel 35

Identifikationsnummer och förteckningar över de organ som anmälts inom ramen för denna förordning

1. Kommissionen ska tilldela varje anmält organ ett identifikationsnummer. Organet ska tilldelas ett enda nummer även om det anmäls i enlighet med flera unionsakter.

2. Kommissionen ska offentliggöra förteckningen över de organ som anmälts i enlighet med denna förordning, inklusive de identifikationsnummer som de har tilldelats 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 de andra medlemsstaterna om alla relevanta ändringar av anmälan av ett anmält organ via det elektroniska anmälningsverktyg som avses i artikel 32.2.

2. De förfaranden som beskrivs i artiklarna 31 och 32 ska tillämpas på utvidgningar av anmälans tillämpningsområde. För andra ändringar av anmälan än utvidgningar av dess tillämpningsområde ska de förfaranden som fastställs i följande punkter tillämpas.

Om ett anmält organ beslutar att upphöra med sin verksamhet avseende bedömning av överensstämmelse, ska det så snart som möjligt och vid planerat upphörande ett år innan det upphör med verksamheten underrätta den anmälande myndigheten och de berörda leverantörerna om detta. Intygen får förbli giltiga under en tillfällig period på nio månader efter det att det anmälda organets verksamhet upphört, under förutsättning att ett annat anmält organ skriftligen har bekräftat att det kommer att ta på sig ansvaret för de AI-system som omfattas av dessa intyg. Det nya anmälda organet ska utföra en fullständig bedömning av de AI-system det gäller före utgången av denna period, innan de utfärdar nya intyg för dem. Om det anmälda organet har upphört med sin verksamhet ska den anmälande myndigheten återkalla utseendet.

3. Om en anmälande myndighet har tillräckliga skäl att anse att ett anmält organ inte längre uppfyller de krav som anges i artikel 33 eller att det inte fullgör sina skyldigheter, ska den anmälande myndigheten, förutsatt att det anmälda organet haft möjlighet att framföra sina synpunkter, beroende på hur allvarlig underlåtenheten att uppfylla kraven eller fullgöra skyldigheterna är, inskränka eller återkalla anmälan tillfälligt eller slutgiltigt. Myndigheten ska omedelbart informera kommissionen och de andra medlemsstaterna om detta.

4. Om utseendet har återkallats tillfälligt, inskränkts eller helt eller delvis dragits tillbaka ska det anmälda organet underrätta de berörda tillverkarna senast inom tio dagar.

5. I händelse av inskränkning, tillfällig återkallelse eller tillbakadragande av en anmälan ska den anmälande myndigheten vidta lämpliga åtgärder för att säkerställa att det berörda anmälda organets dokumentation bevaras och göra denna tillgänglig för de anmälande myndigheterna i andra medlemsstater och för marknadskontrollmyndigheterna på deras begäran.

6. I händelse av inskränkning, tillfällig återkallelse eller tillbakadragande av ett utseende ska den anmälande myndigheten

   a) bedöma inverkan på de intyg som det anmälda organet har utfärdat,

   b) lägga fram en rapport om sina slutsatser för kommissionen och de andra medlemsstaterna senast tre månader efter att ha anmält ändringarna av anmälan,

   c) kräva att det anmälda organet, inom en rimlig tid som myndigheten fastställer, tillfälligt återkallar eller drar tillbaka intyg som utfärdats på felaktiga grunder för att säkerställa överensstämmelse för AI-system på marknaden,

   d) informera kommissionen och medlemsstaterna om intyg för vilka den har krävt tillfällig återkallelse eller tillbakadragande,

e) förse de nationella behöriga myndigheterna i den medlemsstat där leverantören har sitt säte med all relevant information om de intyg för vilka den har begärt tillfällig återkallelse eller tillbakadragande. Denna behöriga myndighet ska vidta lämpliga åtgärder, om så är nödvändigt för att undvika en potentiell risk för hälsa, säkerhet eller grundläggande rättigheter.

7. Med undantag för intyg som utfärdats på felaktiga grunder, och om en anmälan har återkallats tillfälligt eller inskränkts, ska intygen alltjämt vara giltiga i följande fall:

a) Den anmälande myndigheten har inom en månad efter det tillfälliga återkallandet eller inskränkningen bekräftat att det inte finns någon risk för hälsa, säkerhet eller grundläggande rättigheter när det gäller intyg som påverkas av den tillfälliga återkallelsen eller inskränkningen, och den anmälande myndigheten har angett en tidsplan och åtgärder som förväntas för att avhjälpa den tillfälliga återkallelsen eller inskränkningen,

b) Den anmälande myndigheten har bekräftat att inga intyg av betydelse för det tillfälliga återkallandet ska utfärdas, ändras eller utfärdas på nytt under den tid som den tillfälliga återkallelsen eller inskränkningen gäller och anger huruvida det anmälda organet har förmåga att fortsätta att övervaka och ansvara för de befintliga intyg som utfärdats för den period som den tillfälliga återkallelsen eller inskränkningen gäller. Om myndigheten med ansvar för anmälda organ fastställer att det anmälda organet inte har förmåga att stödja befintliga utfärdade intyg,ska leverantören till de nationella behöriga myndigheterna i den medlemsstat där leverantören av det system som omfattas av intyget har sitt säte inom tre månader efter den tillfälliga återkallelsen eller inskränkningen lämna en skriftlig bekräftelse på att ett annat kvalificerat anmält organ tillfälligt tar på sig det anmälda organets uppgifter att övervaka och fortsätta att ansvara för intygen under den period då den tillfälliga återkallelsen eller inskränkningen gäller.

8. Med undantag för intyg som utfärdats på felaktiga grunder och fall där ett utseende har dragits tillbaka ska intygen fortsätta att vara giltiga i nio månader under följande omständigheter:

a) Om 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 och grundläggande rättigheter i samband med systemen i fråga.

b) Ett annat anmält organ har bekräftat skriftligen att det omedelbart kommer att ansvara för dessa system och ha slutfört en bedömning av dem inom tolv månader efter det att utseendet har dragits tillbaka.

I de fall som avses i första stycket får den nationella behöriga myndigheten i den medlemsstat där leverantören av det system som omfattas av intyget har sitt driftsställe förlänga intygens provisoriska giltighet med ytterligare perioder på tre månader, vilka sammanlagt inte får överstiga tolv månader.

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 anmälan ska omedelbart meddela detta till kommissionen, de andra medlemsstaterna och de andra anmälda organen.

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 uppfyller kraven i artikel 33.

2. Den anmälande myndigheten ska på begäran ge kommissionen all information om anmälan av det berörda anmälda organet.

3. Kommissionen ska se till att all konfidentiell information som erhållits i samband med undersökningarna i enlighet med denna artikel behandlas konfidentiellt i enlighet med artikel 70.

4. Om kommissionen konstaterar att ett anmält organ inte uppfyller eller inte längre uppfyller kraven som fastställs i artikel 33 ska den informera den anmälande myndigheten om skälen till detta konstaterande och anmoda den att vidta erforderliga korrigerande åtgärder, inbegripet att vid behov tillfälligt återkalla, inskränka eller dra tillbaka anmälan. Om den anmälande myndigheten inte vidtar erforderliga korrigerande åtgärder får kommissionen genom genomförandeakter tillfälligt återkalla, inskränka eller dra tillbaka anmälan. Den genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 74.2.

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. Den anmälande myndigheten ska se till att de organ som de har anmält deltar i gruppens arbete direkt eller genom utsedda representanter.

Artikel 39

Organ för bedömning av överensstämmelse i tredje länder

Organ för bedömningar av överensstämmelse som inrättats enligt lagstiftningen i ett tredjeland med vilket unionen har ingått ett avtal kan bemyndigas att utföra den verksamhet som bedrivs av anmälda organ enligt denna förordning, förutsatt att de uppfyller kraven i artikel 33.

KAPITEL 5

STANDARDER, BEDÖMNING AV ÖVERENSSTÄMMELSE, INTYG, REGISTRERING

Artikel 40

Harmoniserade standarder

1. AI-system med hög risk eller AI-system för allmänna ändamål som överensstämmer med harmoniserade standarder eller delar av dessa, till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning*, ska förutsättas överensstämma med de krav som fastställs i kapitel 2 i denna avdelning eller, i tillämpliga fall, kraven i artiklarna 4a och 4b, i den omfattning som standarderna omfattar dessa krav.

2. När kommissionen utfärdar en begäran om standardisering till europeiska standardiseringsorganisationer i enlighet med artikel 10 i förordning (EU) nr 1025/2012 ska dess specifikationer innebära att standarderna ska vara enhetliga, tydliga och utformade på ett sådant sätt att de särskilt syftar till att uppfylla följande mål:

   a) Säkerställa att AI-system som släpps ut på marknaden eller tas i bruk i unionen är säkra och respekterar unionens värden samt stärker unionens öppna strategiska oberoende.

   b) Främja investeringar och innovation inom AI, inbegripet genom ökad rättssäkerhet, samt konkurrenskraften och tillväxten på unionsmarknaden.

   c) Främja förvaltningsstrukturer enligt en flerpartsmodell, med företrädare för alla relevanta europeiska berörda parter (till exempel industrin, små och medelstora företag, det civila samhället, forskare).

   d) Bidra till att stärka det globala samarbetet om standardisering på AI-området på ett sätt som är förenligt med unionens värden och intressen.

   Kommissionen ska kräva att de europeiska standardiseringsorganisationerna påvisar att de har gjort sitt yttersta för att uppnå ovannämnda mål.

Artikel 41

Gemensamma specifikationer

1. Kommissionen ska ges befogenhet att, efter samråd med den AI-nämnd som avses i artikel 56, anta genomförandeakter i enlighet med det granskningsförfarande som avses i artikel 74.2 om fastställande av gemensamma tekniska specifikationer för de krav som anges i kapitel 2 i denna avdelning eller, i tillämpliga fall, för de krav som anges i artiklarna 4a och 4b, om följande villkor är uppfyllda:

   a) Ingen hänvisning till harmoniserade standarder som omfattar de relevanta säkerhetsproblemen eller frågorna som rör de grundläggande rättigheterna har offentliggjorts i *Europeiska unionens officiella tidning* i enlighet med förordning (EU) nr 1025/2012.

   b) 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 kapitel 2 i denna avdelning.

   c) Den begäran som avses i led b har inte godtagits av någon av de europeiska standardiseringsorganisationerna. eller de harmoniserade standarder som behandlar begäran har inte lämnats inom den tidsfrist som fastställts i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012, eller dessa standarder överensstämmer inte med begäran.

1a. 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 är uppfyllda.

2. Vid det tidiga utarbetandet av utkastet till genomförandeakt om fastställande av den gemensamma specifikationen ska kommissionen uppfylla de mål som avses i artikel 40.2 och samla in synpunkter från relevanta organ eller expertgrupper som inrättats enligt relevant sektorsspecifik unionslagstiftning. På grundval av detta samråd ska kommissionen utarbeta utkastet till genomförandeakt.

3. AI-system med hög risk eller AI-system för allmänna ändamål som överensstämmer med de gemensamma specifikationer som det hänvisas till i punkt 1 ska förutsättas överensstämma med de krav som fastställs i kapitel 2 i denna avdelning eller, i tillämpliga fall, kraven i artiklarna 4a och 4b, i den omfattning som de gemensamma specifikationerna omfattar dessa krav.

4. När hänvisningar till en harmoniserad standard offentliggörs i *Europeiska unionens officiella tidning* ska de genomförandeakter som avses i punkt 1 och som omfattar kraven i kapitel 2 i denna avdelning eller kraven i artikel 4a och artikel 4b upphävas, beroende på vad som är tillämpligt.

5. Om en medlemsstat anser att en gemensam specifikation inte helt uppfyller kraven i kapitel 2 i denna avdelning eller kraven i artiklarna 4a och 4b, beroende på vad som är tillämpligt, ska den underrätta kommissionen om detta med en detaljerad förklaring, och kommissionen ska bedöma denna information och i lämpliga fall ändra genomförandeakten om fastställande av den gemensamma specifikationen i fråga.

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 och funktionella miljö inom vilken de är avsedda att användas ska antas uppfylla de respektive kraven i artikel 10.4.

2. AI-system med hög risk eller AI-system för allmänna ändamål som har certifierats, eller för vilka en försäkran om överensstämmelse har utfärdats inom ramen för en ordning för cybersäkerhet i enlighet med Europaparlamentets och rådets förordning (EU) 2019/881[33], och till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning*, ska förutsättas överensstämma med de cybersäkerhetskrav som anges i artikel 15 i denna förordning, 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 denne vill visa att ett AI-system med hög risk uppfyller kraven i kapitel 2 i denna avdelning och denne 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:

   a) Det förfarande för bedömning av överensstämmelse grundat på intern kontroll som hänvisas till i bilaga VI.

   b) Det förfarande för bedömning av överensstämmelse grundat på en bedömning av kvalitetsstyrningssystemet och en bedömning av den tekniska dokumentationen, med deltagande av ett anmält organ, som hänvisas till i bilaga VII.

   När leverantören vill visa att ett AI-system med hög risk uppfyller kraven som fastställs i kapitel 2 i denna avdelning och leverantören inte har tillämpat eller endast delvis har tillämpat de harmoniserade standarder som hänvisas till i artikel 40, eller i fall där sådana harmoniserade standarder saknas och de gemensamma specifikationerna som det hänvisas till i artikel 41 inte är tillgängliga, ska leverantören följa det förfarande för bedömning som fastställs i bilaga VII.

[33] 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. 1).

För det förfarande för bedömning av överensstämmelse som avses i bilaga VII får leverantören välja vilket av de anmälda organen som helst. Om systemet är avsett att tas i bruk av brottsbekämpande myndigheter, immigrations- eller asylmyndigheter eller EU:s institutioner, organ eller byråer ska dock den marknadskontrollmyndighet som avses i artikel 63.5 eller 63.6, enligt 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 och för de AI-system för allmänna ändamål som avses i avdelning 1a ska leverantörerna följa det förfarande för bedömning av överensstämmelse grundat på intern kontroll som hänvisas till i bilaga VI, vilket inte föreskriver att ett anmält organ ska involveras.

3. För AI-system med hög risk på vilka de rättsakter som förtecknas i avsnitt A i bilaga II är tillämpliga, ska leverantören följa den relevanta bedömning av överensstämmelse som krävs enligt dessa rättsakter. Kraven i kapitel 2 i denna avdelning ska tillämpas på de AI-systemen med hög risk och ska ingå i den bedömningen. Punkterna 4.3, 4.4, 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 kapitel 2 i denna avdelning, förutsatt att dessa anmälda organs överensstämmelse med kraven i artikel 33.4, 33.9 och 33.10 har bedömts i samband med anmälningsförfarandet inom ramen för dessa rättsakter.

Om de rättsakter som förtecknas i avsnitt A i bilaga II gör det möjligt för tillverkaren av produkten att välja att inte delta i en bedömning av överensstämmelse från tredje part, förutsatt att tillverkaren har tillämpat alla harmoniserade standarder som omfattar alla relevanta krav, kan tillverkaren använda sig av detta alternativ endast om denne också har tillämpat harmoniserade standarder eller, i tillämpliga fall, de gemensamma specifikationer som avses i artikel 41, som omfattar de krav som anges i kapitel 2 i denna avdelning.

4. [utgår]

5. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 73 i syfte att uppdatera bilagorna VI och VII på grund av tekniska framsteg.

6. Kommissionen ges befogenhet att anta delegerade akter för att ändra punkterna 1 och 2 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 berörda 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. På begäran av leverantören får intygets giltighet förlängas med högst fem år i taget på grundval av en ny bedömning i enlighet med det tillämpliga förfarandet för bedömning av överensstämmelse. Eventuella tillägg till ett intyg ska vara giltiga så länge som intyget är giltigt.

3. Om ett anmält organ konstaterar att ett AI-system inte längre uppfyller kraven som fastställs i kapitel 2 i denna avdelning, ska det, med beaktande av proportionalitetsprincipen, tillfälligt återkalla eller dra tillbaka det utfärdade intyget eller införa inskränkningar för det, om efterlevnad av dessa krav inte säkerställs genom lämpliga korrigerande åtgärder vidtagna av systemleverantören inom en rimlig tidsgräns som fastställts av det anmälda organet. Det anmälda organet ska motivera sitt beslut.

Artikel 45

Överklagande av de anmälda organens beslut

Det ska finnas ett förfarande för överklagande av de anmälda organens beslut.

Artikel 46

De anmälda organens informationsskyldighet

1. Anmälda organ ska informera den anmälande myndigheten om följande:

   a) Alla eventuella unionsintyg för bedömning av den tekniska dokumentationen, tillägg till dessa intyg samt godkännanden av kvalitetsstyrningssystem som utfärdats i enlighet med kraven i bilaga VII.

   b) Eventuella avslag, begränsningar, tillfälliga återkallelser eller tillbakadragningar av ett godkännande av kvalitetsstyrningssystem eller av ett unionsintyg för bedömning av den tekniska dokumentationen utfärdade i enlighet med kraven i bilaga VII.

   c) Omständigheter som inverkar på omfattningen av eller villkoren för anmälan.

   d) Begäran 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

   a) godkännanden av kvalitetsstyrningssystem som det har vägrat utfärda eller tillfälligt återkallat eller dragit tillbaka och, på begäran, om godkännanden av kvalitetssystem som det har utfärdat,

b) EU-intyg för bedömning av den tekniska dokumentationen eller tillägg till dessa intyg som det har avslagit, tillfälligt återkallat eller dragit tillbaka eller på annat sätt belagt med restriktioner 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 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 1–3 ska fullgöras i enlighet med artikel 70.

Artikel 47

Undantag från förfarandena för bedömning av överensstämmelse

1. Genom undantag från artikel 43 och på vederbörligen motiverad begäran får vilken marknadskontrollmyndighet som helst tillåta att specifika AI-system med hög risk släpps ut på marknaden eller tas i bruk inom den berörda medlemsstatens territorium, av exceptionella skäl som rör allmän säkerhet eller skydd av människors liv och hälsa, miljöskydd och skydd av viktiga industriella och infrastrukturella tillgångar. Tillståndet ska gälla under en begränsad tid, 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.

1a. 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, och om ett sådant tillstånd avslås ska dess användning upphöra med omedelbar verkan, och alla resultat och utdata från denna användning ska omedelbart kasseras.

2. Det godkännande som avses i punkt 1 ska endast utfärdas om marknadskontrollmyndigheten konstaterar att AI-systemet med hög risk uppfyller kraven i kapitel 2 i denna avdelning. Marknadskontrollmyndigheten ska informera kommissionen och de andra medlemsstaterna om eventuella godkännanden som utfärdats i enlighet med punkt 1. Denna skyldighet ska inte omfatta känsliga operativa uppgifter som rör de brottsbekämpande myndigheternas verksamhet.

3. [utgår]

4. [utgår]

5. [utgår]

6. För AI-system med hög risk som är relaterade till produkter som omfattas av den unionslagstiftning om harmonisering som avses i bilaga II avsnitt A ska endast de undantagsförfaranden för bedömning av överensstämmelse som fastställs i den lagstiftningen tillämpas.

Artikel 48

EU-försäkran om överensstämmelse

1. Leverantören ska upprätta en skriftlig eller elektroniskt undertecknad EU-försäkran om överensstämmelse för varje AI-system och kunna uppvisa den för de nationella myndigheterna i tio år efter det att AI-systemet har släppts ut på marknaden eller tagits i bruk. I EU-försäkran om överensstämmelse ska det anges för vilket AI-system den har upprättats. 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 kapitel 2 i denna avdelning. 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 den eller de medlemsstater där AI-systemet med hög risk tillhandahålls.

3. Om AI-system med hög risk omfattas av annan harmoniseringslagstiftning i unionen som också kräver en EU-försäkran om överensstämmelse ska en enda EU-försäkran om överensstämmelse upprättas med avseende på all unionslagstiftning som är tillämplig på AI-systemet med hög risk. Försäkran ska innehålla all information som krävs för att identifiera vilken harmoniseringslagstiftning som försäkran gäller.

4. Genom att upprätta EU-försäkran om överensstämmelse ska leverantören ta på sig ansvaret för att kraven som fastställs i kapitel 2 i denna avdelning uppfylls. Leverantören ska hålla EU-försäkran om överensstämmelse uppdaterad i enlighet med behov.

5. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 73 i syfte av att uppdatera innehållet i den EU-försäkran om överensstämmelse som inrättas i bilaga V för att introducera element som blir nödvändiga på grund av tekniska framsteg.

Artikel 49

CE-märkning om överensstämmelse

1. CE-märkningen om överensstämmelse ska omfattas av de allmänna principer som fastställs i artikel 30 i förordning (EG) nr 765/2008.

2. CE-märkningen ska anbringas på AI-systemet med hög risk så att den är synlig, läsbar och outplånlig. Om detta inte är möjligt eller lämpligt på grund av arten av AI-systemet med hög risk, ska märkningen anbringas på förpackningen eller på den medföljande dokumentationen, beroende på vad som är lämpligt.

3. CE-märkningen ska i tillämpliga fall åtföljas av identifikationsnumret för det anmälda organ som ansvarar för den bedömning av överensstämmelse som föreskrivs i artikel 43. Identifikationsnumret ska också anges i sådant reklammaterial där det nämns att AI-systemet med hög risk uppfyller kraven för CE-märkning.

Artikel 50

[utgår]

Artikel 51

Registrering av berörda operatörer och av AI-system med hög risk som förtecknas i bilaga III

1. Med undantag för AI-system med hög risk som avses i punkterna 1, 6 och 7 i bilaga III på områdena för brottsbekämpning och förvaltning av migration, asyl och gränskontroll, samt AI-system med hög risk som avses i punkt 2 i bilaga III, ska leverantören och, i tillämpliga fall, ombudet registrera sig i den EU-databas som avses i artikel 60 innan ett AI-system med hög risk som förtecknas i bilaga III släpps ut på marknaden eller tas i bruk. Leverantören eller, i tillämpliga fall, ombudet ska också registrera sina system i den databasen.

2. Innan ett AI-system med hög risk som förtecknas i bilaga III används ska användare av AI-system med hög risk som är offentliga myndigheter, byråer eller organ, eller enheter som agerar på deras vägnar, registrera sig i den EU-databas som avses i artikel 60 och välja det system som de avser att använda.

   De skyldigheter som fastställs i föregående stycke ska inte tillämpas på brottsbekämpande myndigheter, byråer eller organ eller myndigheter, byråer eller organ för gränskontroll, immigration och asyl och myndigheter, byråer eller organ som använder AI-system med hög risk som avses i punkt 2 i bilaga III, liksom enheter som agerar på deras vägnar.

AVDELNING IV

TRANSPARENSKRAV FÖR LEVERANTÖRER OCH ANVÄNDARE AV VISSA AI-SYSTEM

Artikel 52

Transparenskrav för leverantörer och användare av vissa AI-system

1. Leverantörer ska säkerställa att AI-system som är avsedda att interagera med fysiska personer utformas och utvecklas på ett sådant sätt att fysiska personer 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 och 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. Användare av system för biometrisk kategorisering ska informera de fysiska personer som exponeras för systemet om systemets drift. Denna skyldighet ska inte gälla AI-system som används för biometrisk kategorisering som enligt lag får upptäcka, förebygga och utreda brott, med förbehåll för lämpliga garantier för tredje mans rättigheter och friheter.

2a. Användare av system för känsloigenkänning ska informera de fysiska personer som exponeras för systemet om systemets drift. Denna skyldighet ska inte gälla AI-system som används för känsloigenkänning som enligt lag får upptäcka, förebygga och utreda brott, med förbehåll för lämpliga garantier för tredje mans rättigheter och friheter.

3. Användare av ett AI-system som genererar eller manipulerar bilder eller ljud eller videoinnehåll som på ett märkbart sätt liknar befintliga personer, objekt, platser eller andra enheter eller händelser och som för en person felaktigt skulle framstå som autentiska (deepfake), ska upplysa om att innehållet har skapats artificiellt eller manipulerats.

Första stycket ska dock inte tillämpas om användningen enligt lag är tillåten för att upptäcka, förhindra, utreda och lagföra brott eller om innehållet ingår i ett uppenbart kreativt, satiriskt, konstnärligt eller fiktivt verk eller program, med förbehåll för lämpliga garantier för tredje mans rättigheter och friheter.

3a. Den information som avses i punkterna 1–3 ska lämnas till fysiska personer på ett tydligt och urskiljbart sätt senast vid tidpunkten för den första interaktionen eller exponeringen.

4. Punkterna 1, 2, 2a, 3 och 3a ska inte påverka de krav och skyldigheter som fastställs i avdelning III i denna förordning och ska inte påverka andra transparensskyldigheter för användare av AI-system som fastställs i unionsrätten eller nationell rätt.

AVDELNING V

ÅTGÄRDER TILL STÖD FÖR INNOVATION

Artikel 53

Regulatoriska sandlådor för AI

-1a. Nationella behöriga myndigheter får inrätta regulatoriska sandlådor för AI för utveckling, träning, testning och validering av innovativa AI-system under direkt tillsyn, vägledning och stöd av den nationella behöriga myndigheten, innan dessa system släpps ut på marknaden eller tas i bruk. Sådana regulatoriska sandlådor får omfatta tester under verkliga förhållanden som övervakas av de nationella behöriga myndigheterna.

-1b. [utgår]

-1c. I lämpliga fall ska de nationella behöriga myndigheterna samarbeta med andra relevanta myndigheter, och de får tillåta deltagande av andra aktörer inom AI-ekosystemet.

-1d. Denna artikel ska inte påverka andra regulatoriska sandlådor som inrättats enligt nationell rätt eller unionsrätten, inbegripet i fall där de produkter eller tjänster som testas i dem är kopplade till användningen av innovativa AI-system. Medlemsstaterna ska säkerställa lämpligt samarbete mellan de myndigheter som övervakar dessa andra sandlådor och de nationella behöriga myndigheterna.

1. [utgår]

1a. [utgår]

1b. Inrättandet av regulatoriska sandlådor för AI enligt denna förordning ska syfta till att bidra till ett eller flera av följande mål:

a) Främja innovation och konkurrenskraft och underlätta utvecklingen av ett AI-ekosystem.
b) Underlätta och påskynda tillgången till unionsmarknaden för AI-system, särskilt när de tillhandahålls av små och medelstora företag, inbegripet nystartade företag.
c) Förbättra rättssäkerheten och bidra till utbyte av bästa praxis genom samarbete med de myndigheter som är involverade i den regulatoriska sandlådan för AI i syfte att säkerställa framtida efterlevnad av denna förordning och, när så är lämpligt, med annan unionslagstiftning och medlemsstaternas lagstiftning.
d) Bidra till evidensbaserat regulatoriskt lärande.

2. [utgår]

2a. Åtkomsten till regulatoriska sandlådor för AI ska vara öppen för alla leverantörer eller potentiella leverantörer av ett AI-system som uppfyller de behörighets- och urvalskriterier som avses i punkt 6 a och som har valts ut av de nationella behöriga myndigheterna efter det urvalsförfarande som avses i punkt 6 b. Leverantörer eller potentiella leverantörer får också lämna in ansökningar i partnerskap med användare eller andra relevanta tredje parter.

Deltagandet i den regulatoriska sandlådan för AI ska begränsas till en period som är lämplig med hänsyn till projektets komplexitet och omfattning. Denna period får förlängas av den nationella behöriga myndigheten.

Deltagande i den regulatoriska sandlådan för AI ska baseras på en särskild plan som avses i punkt 6 i denna artikel och som ska överenskommas mellan deltagaren/deltagarna och de nationella behöriga myndigheterna, beroende på vad som är tillämpligt.

3. De regulatoriska sandlådorna för AI ska inte påverka tillsynsbefogenheterna eller de korrigerande befogenheterna för de myndigheter som utövar tillsyn över sandlådan. Dessa myndigheter ska utöva sina tillsynsbefogenheter på ett flexibelt sätt inom ramen för den relevanta lagstiftningen, 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.

Förutsatt att deltagaren/deltagarna respekterar sandlådeplanen och villkoren för deras deltagande enligt punkt 6 c och i god tro följer myndigheternas vägledning, ska inga administrativa sanktionsavgifter åläggas av myndigheterna för överträdelse av tillämplig unionslagstiftning eller medlemsstatslagstiftning om det AI-system som är föremål för tillsyn i sandlådan, inbegripet bestämmelserna i denna förordning.

4. Deltagarna förblir ansvariga enligt tillämplig unionslagstiftning och medlemsstaternas tillämpliga lagstiftning om ansvar för eventuella skador som orsakas under deras deltagande i en regulatorisk sandlåda för AI.

4a. På begäran av leverantören eller den potentiella leverantören av AI-systemet ska den nationella behöriga myndigheten i tillämpliga fall tillhandahålla ett skriftligt bevis på den verksamhet som framgångsrikt utförts i sandlådan. Den nationella behöriga myndigheten ska också tillhandahålla en slutrapport med uppgifter om den verksamhet som bedrivs i sandlådan och tillhörande resultat och läranderesultat. Sådana skriftliga bevis och slutrapporter får beaktas av marknadskontrollmyndigheter eller anmälda organ, beroende på vad som är tillämpligt, i samband med förfaranden för bedömning av överensstämmelse eller verifiering för marknadskontroll.

Om inte annat följer av konfidentialitetsbestämmelserna i artikel 70 och med godkännande från deltagarna i sandlådan ska Europeiska kommissionen och AI-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 deltagaren och den nationella behöriga myndigheten uttryckligen samtycker till detta kan slutrapporten offentliggöras via den enda informationsplattform som avses i artikel 55.3 b.

4b. De regulatoriska sandlådorna för AI ska utformas och genomföras på ett sådant sätt att de, i förekommande fall, underlättar gränsöverskridande samarbete mellan de nationella behöriga myndigheterna.

5. De nationella behöriga myndigheterna ska offentliggöra årliga rapporter om genomförandet av de regulatoriska sandlådorna för AI, inbegripet god praxis, tillvaratagna erfarenheter och rekommendationer om deras etablering och, i tillämpliga fall, om tillämpningen av denna förordning och annan unionslagstiftning som övervakas inom sandlådan. Dessa årliga rapporter ska överlämnas till AI-nämnden, som ska offentliggöra en sammanfattning av all god praxis samt alla tillvaratagna erfarenheter och rekommendationer. Denna skyldighet att offentliggöra årsrapporter ska inte omfatta känsliga operativa uppgifter som rör brottsbekämpande myndigheters, gränskontrollmyndigheters samt invandrings- eller asylmyndigheters verksamhet. Kommissionen och AI-nämnden ska, när så är lämpligt, beakta årsrapporterna när de utför sina uppgifter enligt denna förordning.

5b. Kommissionen ska säkerställa att information om regulatoriska sandlådor för AI, inbegripet sådana som inrättats enligt denna artikel, finns tillgänglig via den enda informationsplattform som avses i artikel 55.3 b.

6. Formerna och villkoren för inrättande och drift av regulatoriska sandlådor för AI enligt denna förordning ska antas genom genomförandeakter i enlighet med det granskningsförfarande som avses i artikel 74.2.

Formerna och villkoren ska i största möjliga utsträckning stödja flexibilitet för nationella behöriga myndigheter att inrätta och driva sina regulatoriska sandlådor för AI, främja innovation och regulatoriskt lärande och ska särskilt beakta de deltagande små och medelstora företagens, inbegripet nystartade företags, särskilda omständigheter och kapacitet.

Dessa genomförandeakter ska innehålla gemensamma huvudprinciper i följande frågor:

a) Behörighet och urval 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.

7. När nationella behöriga myndigheter överväger att godkänna testning under verkliga förhållanden som står under tillsyn inom ramen för en regulatorisk sandlåda för AI som inrättats 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 54

Ytterligare behandling av personuppgifter för utveckling av vissa AI-system i allmänhetens intresse i den regulatoriska sandlådan för AI

1. I den regulatoriska sandlådan för AI får personuppgifter som lagligen samlats in för andra ändamål behandlas i syfte att utveckla, testa och träna innovativa AI-system i sandlådan på följande kumulativa villkor:

   a) En offentlig myndighet eller en annan fysisk eller juridisk person som lyder under offentlig rätt eller privaträtt ska utveckla de innovativa AI-systemen för att skydda ett väsentligt allmänintresse på ett eller flera av följande områden:

      i) [utgår]

      ii) Allmän säkerhet och hälsa, inbegripet förebyggande, kontroll och behandling av sjukdomar och förbättring av hälso- och sjukvårdssystemen.

      iii) Skydd och förbättring av miljöns kvalitet, inbegripet grön omställning, begränsning av och anpassning till klimatförändringar.

      iv) Energihållbarhet, transport och mobilitet.

      v) Den offentliga förvaltningens och de offentliga tjänsternas effektivitet och kvalitet.

      vi) Cybersäkerhet och kritiska entiteters motståndskraft.

   b) De data som behandlas är nödvändiga för att uppfylla ett eller flera av de krav som avses i avdelning III kapitel 2 i fall där dessa krav inte kan uppfyllas effektivt genom behandling av anonymiserade eller syntetiska data eller andra data som inte är 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 deltagarnas kontroll och endast behöriga personer har tillgång till dessa uppgifter.

e) Inga personuppgifter som behandlas får överlämnas, överföras eller på annat sätt göras tillgängliga för andra parter som inte är deltagare i sandlådan, såvida inte ett sådant utlämnande sker i enlighet med förordning (EU) 2016/679 eller, i tillämpliga fall, förordning 2018/725, och alla deltagare har samtyckt till det.

f) Behandling av personuppgifter i samband med sandlådan ska inte påverka tillämpningen av de registrerades rättigheter enligt unionslagstiftningen om skydd av personuppgifter, särskilt artikel 22 i förordning (EU) 2016/679 och artikel 24 i förordning (EU) 2018/1725.

g) Alla personuppgifter som behandlas inom ramen för sandlådan ska skyddas genom lämpliga tekniska och organisatoriska åtgärder och raderas när deltagandet i sandlådan har upphört 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 dokumentationen 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 samt invandrings- eller asylmyndigheters verksamhet.

1a. I syfte 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, under brottsbekämpande myndigheters överinseende och ansvar, ska behandlingen av personuppgifter i regulatoriska sandlådor för AI baseras på en specifik medlemsstats lagstiftning eller unionslagstiftning och omfattas av samma kumulativa villkor som avses i punkt 1.

2. Punkt 1 ska inte påverka tillämpningen av unionslagstiftning eller medlemsstatslagstiftning om grunden för behandling av personuppgifter som är nödvändig för att utveckla, testa och träna innovativa AI-system eller någon annan rättslig grund, i enlighet med unionslagstiftningen om skydd av personuppgifter.

Artikel 54a

Testning av AI-system med hög risk under verkliga förhållanden utanför regulatoriska sandlådor för AI

1. Testning av AI-system 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 bestämmelserna i denna artikel och den plan för testning under verkliga förhållanden som avses i denna artikel.

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 74.2.

Denna bestämmelse ska inte påverka tillämpningen av unionslagstiftningen eller medlemsstaternas lagstiftning 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 II.

2. Leverantörer eller potentiella leverantörer får på egen hand eller i partnerskap med en eller flera potentiella användare utföra testning av AI-system med hög risk som avses i bilaga III under verkliga förhållanden 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 den etiska granskning som får krävas 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 eller de medlemsstater där testningen under verkliga förhållanden ska utföras.

b) Marknadskontrollmyndigheten i den eller de medlemsstater där testningen under verkliga förhållanden ska utföras har inte invänt mot testningen inom 30 dagar efter det att den lämnats in.

c) Leverantören eller den potentiella leverantören har, med undantag för 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, registrerat testning under verkliga förhållanden i den EU-databas som avses i artikel 60.5a med ett enda unionsomfattande identifieringsnummer och den information som anges i bilaga VIIIa.

d) Den leverantör eller potentiella leverantör som utför testningen under verkliga förhållanden är etablerad i unionen eller har utsett ett ombud för testning under verkliga förhållanden som är etablerat i unionen.

e) Uppgifter som samlas in och behandlas för testning under verkliga förhållanden ska inte överföras till länder utanför unionen, såvida inte överföringen och behandlingen ger garantier som är likvärdiga med dem som föreskrivs i unionsrätten.

f) Testningen under verkliga förhållanden varar inte längre än vad som är nödvändigt för att uppnå dess mål och under inga omständigheter längre än 12 månader.

g) Personer som tillhör utsatta grupper på grund av ålder eller fysisk eller psykisk funktionsnedsättning skyddas på lämpligt sätt.

h) [utgår]

i) Om en leverantör eller potentiell leverantör organiserar testningen under verkliga förhållanden i samarbete med en eller flera potentiella användare, har dessa informerats om alla aspekter av testningen som är relevanta för deras beslut att delta och fått relevanta instruktioner om hur det AI-system som avses i artikel 13 ska användas. Leverantören eller den potentiella leverantören och användaren/användarna 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 annan tillämplig unionslagstiftning och medlemsstatslagstiftning.

j) Försökspersonerna i testningen under verkliga förhållanden har gett sitt informerade samtycke i enlighet med artikel 54b, eller, när det gäller brottsbekämpning, får själva testningen och resultatet av testningen under verkliga förhållanden, om en begäran om informerat samtycke skulle hindra AI-systemet från att testas, inte ha negativ inverkan på försökspersonen.

k) Testningen under verkliga förhållanden övervakas effektivt av leverantören eller den potentiella leverantören och användaren/användarna genom personer som har lämpliga kvalifikationer inom det berörda området och som har den kapacitet, utbildning och befogenhet som krävs för att utföra sina uppgifter.

l) AI-systemets förutsägelser, rekommendationer eller beslut får upphävas eller ignoreras.

5. Varje försöksperson inom testningen under verkliga förhållanden, eller dennes 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 återkalla sitt informerade samtycke. Tillbakadragandet av det informerade samtycket ska inte påverka den verksamhet som redan utförts och användningen av uppgifter som erhållits på grundval av det informerade samtycket innan det drogs tillbaka.

6. Alla allvarliga incidenter som identifieras under testningen under verkliga förhållanden ska rapporteras till den nationella marknadskontrollmyndigheten i enlighet med artikel 62 i denna förordning. Leverantören eller den potentiella leverantören ska vidta omedelbara riskreducerande åtgärder eller, om så inte är fallet, tillfälligt avbryta testningen under verkliga förhållanden tills sådan riskreducering äger rum eller i annat fall avsluta den. Leverantören eller den potentiella leverantören ska inrätta ett förfarande för snabb återkallelse av AI-systemet när testningen under verkliga förhållanden avslutas på detta sätt.

7. Leverantörer eller potentiella leverantörer ska underrätta den nationella marknadskontrollmyndigheten i den eller de medlemsstater där testningen under verkliga förhållanden ska utföras om det tillfälliga avbrottet eller avslutandet av testningen under verkliga förhållanden och de slutliga resultaten.

8. Leverantören och den potentiella leverantören ska vara ansvariga enligt tillämplig unionslagstiftning och medlemsstaternas lagstiftning om ansvar för eventuella skador som orsakas under deras deltagande i testningen under verkliga förhållanden.

Artikel 54b

Informerat samtycke till deltagande i testning under verkliga förhållanden utanför regulatoriska sandlådor för AI

1. För testning under verkliga förhållanden enligt artikel 54a ska informerat samtycke ges frivilligt av försökspersonen innan han eller hon deltar i sådan testning och efter att ha vederbörligen informerats med koncis, tydlig, relevant och begriplig information om

i) den karaktär och de mål som testningen under verkliga förhållanden har och de eventuella olägenheter som kan vara förknippade med att delta,

ii) de förhållanden under vilken testningen under verkliga förhållanden ska utföras, inbegripet den förväntade varaktigheten för försökspersonens deltagande,

iii) försökspersonens rättigheter och garantier avseende deltagandet, särskilt försökspersonens rätt att vägra att delta i och rätten att när som helst avsluta sitt deltagande i testningen under verkliga förhållanden utan negativa följder och utan att behöva motivera sitt beslut,

iv) formerna för begäran om upphävande eller ignorerande av AI-systemets förutsägelser, rekommendationer eller beslut,

v) det enda unionsomfattande identifikationsnumret för testningen under verkliga förhållanden i enlighet med artikel 54a.4c och kontaktuppgifter för leverantören eller dennes ombud från vilket ytterligare information kan erhållas.

2. Det informerade samtycket ska dateras och dokumenteras och en kopia ska ges till försökspersonen eller dennes rättsliga ombud.

Artikel 55

Stödåtgärder för operatörer, särskilt små och medelstora företag, inbegripet nystartade företag

1. Medlemsstaterna ska vidta följande åtgärder:

a) Ge små och medelstora företag, inbegripet nystartade företag, prioriterad åtkomst till de regulatoriska sandlådorna för AI, i den mån de uppfyller behörighets- och urvalskriterierna.

b) Anordna särskilda medvetandehöjande åtgärder och utbildning om tillämpningen av denna förordning som är anpassade till behoven hos små och medelstora företag, inbegripet nystartade företag, och lokala, om lämpligt, offentliga myndigheter.

c) När så är lämpligt inrätta en särskild kanal för kommunikation med små och medelstora företag, inbegripet nystartade företag, och, om lämpligt, lokala myndigheter, för att ge råd och svara på frågor om genomförandet av denna förordning, inbegripet när det gäller deltagande i regulatoriska sandlådor för AI.

2. De särskilda intressen och behov som små och medelstora företag, inbegripet nystartade företag, har 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. Kommissionen ska vidta följande åtgärder:

(a) På begäran av AI-nämnden tillhandahålla standardiserade mallar för de områden som omfattas av denna förordning.

(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 55a

Undantag för särskilda operatörer

1. De skyldigheter som fastställs i artikel 17 i denna förordning ska inte gälla mikroföretag enligt definitionen i artikel 2.3 i bilagan till kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag, förutsatt att dessa företag inte har partnerföretag eller anknutna företag enligt definitionen i artikel 3 i samma bilaga.

2. Punkt 1 ska inte tolkas som att den undantar dessa aktörer från att uppfylla andra krav och skyldigheter som fastställs i denna förordning, inbegripet dem som fastställs i artiklarna 9, 61 och 62.

3. De krav och skyldigheter för AI-system för allmänna ändamål som fastställs i artikel 4b ska inte tillämpas på mikroföretag samt små och medelstora företag, förutsatt att dessa företag inte har partnerföretag eller anknutna företag enligt definitionen i artikel 3 i bilagan till kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag.

AVDELNING VI

STYRNING

KAPITEL 1

DEN EUROPEISKA NÄMNDEN FÖR ARTIFICIELL INTELLIGENS

Artikel 56

Inrättande av och strukturen för den europeiska nämnden för artificiell intelligens

1. En europeisk nämnd för artificiell intelligens (*nämnden*) inrättas.

2. Nämnden ska bestå av en företrädare per medlemsstat. Europeiska datatillsynsmannen ska delta som observatör. Även kommissionen 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.

2a. Varje företrädare ska utses av sin medlemsstat för en period på tre år som kan förnyas en gång.

2aa. Medlemsstaterna ska se till att deras företrädare i nämnden

   i) har relevant behörighet och relevanta befogenheter i sin medlemsstat för att aktivt bidra till fullgörandet av styrelsens uppgifter enligt artikel 58,

   ii) utses till gemensam kontaktpunkt gentemot styrelsen och när så är lämpligt, med beaktande av medlemsstaternas behov, till gemensam kontaktpunkt för de berörda parterna,

iii) 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.

3. Medlemsstaternas utsedda företrädare ska anta nämndens arbetsordning med två tredjedels majoritet.

Arbetsordningen ska särskilt föreskriva förfaranden för urvalsprocessen, mandatets varaktighet och specificering av ordförandens uppgifter, omröstningsregler och organisationen av nämndens verksamhet och arbetsgrupper.

Nämnden ska inrätta en ständig arbetsgrupp som ska fungera som en plattform för berörda parter och ge råd till nämnden i alla frågor som rör genomförandet av denna förordning, inbegripet utarbetandet av genomförandeakter och delegerade akter. I detta syfte ska organisationer som företräder intressena för leverantörer och användare av AI-system, inbegripet små och medelstora företag och nystartade företag, samt organisationer i det civila samhället, företrädare för berörda personer, forskare, standardiseringsorganisationer, anmälda organ, laboratorier och test- och experimentanläggningar bjudas in att delta i denna arbetsgrupp. Nämnden ska 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.

Nämnden får inrätta andra ständiga eller tillfälliga arbetsgrupper när så är lämpligt i syfte att granska specifika frågor. I lämpliga fall får de berörda parter som avses i föregående stycke bjudas in till sådana arbetsgrupper eller till särskilda möten i dessa undergrupper i egenskap av observatörer.

3a. Nämnden ska vara organiserad och fungera på ett sådant sätt att objektiviteten och opartiskheten i dess verksamhet skyddas.

4. En av företrädarna för medlemsstaterna ska vara ordförande i nämnden. På begäran av ordföranden ska kommissionen sammankalla till möten och förbereda dagordningen i enlighet med nämndens uppdrag enligt denna förordning och nämndens arbetsordning. Kommissionen ska tillhandahålla administrativt och analytiskt stöd till nämndens verksamhet i enlighet med denna förordning.

Artikel 57

[utgår]

Artikel 58

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) samla in och utbyta teknisk och regleringsmässig sakkunskap och bästa praxis bland medlemsstaterna,

b) 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 47, de regulatoriska sandlådornas funktion och testning under verkliga förhållanden enligt artiklarna 53, 54 och 54a,

c) 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 tekniska specifikationer eller befintliga standarder avseende de krav som anges i avdelning III kapitel 2,

   ii) om användning av harmoniserade standarder eller gemensamma specifikationer som avses i artiklarna 40 och 41,

iii) om utarbetande av vägledande handlingar, inbegripet de riktlinjer för fastställande av administrativa sanktionsavgifter som avses i artikel 71.

d) ge kommissionen råd om det potentiella behovet av att ändra bilaga III i enlighet med artiklarna 4 och 7, med beaktande av relevanta tillgängliga bevis och den senaste teknikutvecklingen,

e) ge kommissionen råd under utarbetandet av delegerade akter eller genomförandeakter i enlighet med denna förordning,

f) vid behov samarbeta med relevanta EU-organ, expertgrupper och nätverk, särskilt på områdena produktsäkerhet, cybersäkerhet, konkurrenskraft, digitala tjänster och medietjänster, finansiella tjänster, kryptovalutor, konsumentskydd, dataskydd och skydd av grundläggande rättigheter,

g) bidra till och ge relevant rådgivning till kommissionen vid utarbetandet av den vägledning som avses i artikel 58a eller begära att sådan vägledning utarbetas,

h) att bistå marknadskontrollmyndigheternas arbete och, i samarbete och efter överenskommelse med de berörda marknadskontrollmyndigheterna, främja och stödja gränsöverskridande marknadskontrollsutredningar, bland annat när det gäller uppkomsten av systemrisker som kan uppstå till följd av AI-system,

i) bidra till bedömningen av utbildningsbehoven för personal från medlemsstater som deltar i genomförandet av denna förordning,

j) ge kommissionen råd i internationella frågor om artificiell intelligens.

KAPITEL 1A

RIKTLINJER FRÅN KOMMISSIONEN

Artikel 58a

Riktlinjer från kommissionen om genomförandet av denna förordning

1. På begäran av medlemsstaterna eller nämnden, eller på eget initiativ, ska kommissionen utfärda riktlinjer om det praktiska genomförandet av denna förordning, särskilt om

   i) tillämpningen av de krav som avses i artikel 8–15,

   ii) de förbjudna tillämpningar som avses i artikel 5,

   iii) det praktiska genomförandet av bestämmelserna om väsentliga ändringar,

   iv) det praktiska genomförandet av de enhetliga villkor som avses i artikel 6.3, inbegripet exempel som rör AI-system med hög risk som avses i bilaga III,

   v) det praktiska genomförandet av skyldigheter till transparens som fastställs i artikel 52,

   vi) förhållandet mellan denna förordning och annan relevant unionslagstiftning, bland annat vad gäller konsekvens i kontrollen av efterlevnaden.

När kommissionen utfärdar sådana riktlinjer ska den särskilt uppmärksamma behoven hos små och medelstora företag, inbegripet nystartade företag, lokala offentliga myndigheter och sektorer som mest sannolikt kommer att beröras av denna förordning.

KAPITEL 2

NATIONELLA BEHÖRIGA MYNDIGHETER

Artikel 59

Utseende av nationella behöriga myndigheter

1. [utgår]

2. Varje medlemsstat ska vid tillämpning av denna förordning inrätta eller utse minst en anmälande myndighet och minst en marknadskontrollmyndighet till nationella behöriga myndigheter. Nationella behöriga myndigheter ska vara organiserade och fungera på ett sådant sätt att deras verksamhet och uppgifter skyddas vad avses principerna om objektivitet och opartiskhet. Förutsatt att dessa principer respekteras får sådan verksamhet och sådana uppgifter utföras av en eller flera utsedda myndigheter, i enlighet med medlemsstatens organisatoriska behov.

3. Medlemsstaterna ska underrätta kommissionen om vilken eller vilka myndigheter de har utsett.

4. Medlemsstaterna ska se till att de nationella behöriga myndigheterna har ekonomiska resurser, teknisk utrustning och välkvalificerade mänskliga resurser i tillräcklig omfattning för att kunna fullgöra sina uppgifter enligt denna förordning.

5. Senast *[ett år efter denna förordnings ikraftträdande]* och därefter sex månader före den tidsfrist som avses i artikel 84.2 ska medlemsstaterna informera kommissionen om de nationella behöriga myndigheternas ekonomiska resurser, tekniska utrustning och mänskliga resurser med en bedömning av deras resurstillräcklighet. Kommissionen ska översända denna information till nämnden för diskussion och eventuella rekommendationer.

6. Kommissionen ska underlätta utbytet av erfarenhet mellan nationella behöriga myndigheter.

7. Nationella behöriga myndigheter får ge råd om genomförandet av denna förordning, inbegripet skräddarsydda till små och medelstora företag, inbegripet nystartade företag. När nationella behöriga myndigheter tänker ge vägledning och rådgivning om ett AI-system på områden som omfattas av annan unionslagstiftning, ska de behöriga nationella myndigheterna enligt den unionslagstiftningen i lämpliga fall rådfrågas. Medlemsstaterna får också inrätta en central kontaktpunkt för kommunikation med operatörer.

8. När unionens institutioner, byråer och organ omfattas av denna förordning ska Europeiska datatillsynsmannen fungera som behörig tillsynsmyndighet för dessa.

AVDELNING VII

EU-DATABAS FÖR AI-SYSTEM MED HÖG RISK SOM FÖRTECKNAS I BILAGA III

Artikel 60

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 punkt 2 om berörda operatörer och AI-system med hög risk förtecknade i bilaga III som är registrerade i enlighet med artiklarna 51 och 54a. När kommissionen fastställer funktionspecifikationerna för en sådan databas ska den samråda med AI-nämnden.

2. De uppgifter som förtecknas i del I i bilaga VIII ska föras in i EU-databasen av leverantörerna, ombuden och de relevanta användarna, beroende på vad som är tillämpligt, vid deras registrering. De uppgifter som förtecknas i punkterna 1–11 i bilaga VIII del II ska föras in i EU-databasen av leverantörerna, eller i tillämpliga fall av ombudet, i enlighet med artikel 51. De uppgifter som avses i punkt 12 i bilaga VIII del II ska genereras automatiskt av databasen på grundval av den information som lämnats av berörda användare i enlighet med artikel 51.2. De uppgifter som förtecknas i bilaga VIIIa ska föras in i databasen av de potentiella leverantörerna eller leverantörerna i enlighet med artikel 54a.

3. [utgår]

4. EU-databasen ska inte innehålla några personuppgifter, med undantag för den information som förtecknas i bilaga VIII, och ska inte påverka tillämpningen av artikel 70.

5. Kommissionen ska vara personuppgiftsansvarig för EU-databasen. Den ska göra tillräckligt tekniskt och administrativt stöd tillgängligt för leverantörer, potentiella leverantörer och användare.

5a. Information i EU-databasen som registrerats i enlighet med artikel 51 ska vara tillgänglig för allmänheten. Den information som registreras i enlighet med artikel 54a 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.

AVDELNING VIII

ÖVERVAKNING EFTER UTSLÄPPANDE PÅ MARKANDEN, INFORMATIONSDELNING OCH MARKNADSKONTROLL

KAPITEL 1

ÖVERVAKNING EFTER UTSLÄPPANDE PÅ MARKNADEN

Artikel 61

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 utsläppandet på marknaden på ett sätt som står i proportion till riskerna med AI-systemet med hög risk.

2. För att göra det möjligt för leverantören att utvärdera AI-systemens överensstämmelse med kraven i avdelning III kapitel 2 under hela deras livscykel ska systemet för övervakning efter utsläppande på marknaden samla in, dokumentera och analysera relevanta data som får tillhandahållas av användare eller som får samlas in via andra källor vad gäller hur AI-systemen med hög risk presterar. Denna skyldighet ska inte omfatta känsliga operativa uppgifter om användare av AI-system 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.

4. För AI-system med hög risk som omfattas av de rättsakter som avses i bilaga II avsnitt A, där ett system och en plan för övervakning efter utsläppande på marknaden redan har inrättats enligt den lagstiftningen, ska den dokumentation om övervakningen efter utsläppandet på marknaden anses tillräcklig, förutsatt att den förlaga som avses i punkt 3 används.

Första stycket 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 deras interna styrelseformer, arrangemang eller processer enligt unionslagstiftningen om finansiella tjänster.

KAPITEL 2

INFORMATIONSDELNING OM ALLVARLIGA INCIDENTER

Artikel 62

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.

En sådan underrättelse 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 leverantörerna fått kännedom om den allvarliga incidenten.

2. 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 64.3. Kommissionen ska utarbeta särskilda riktlinjer för att underlätta fullgörandet av de skyldigheter som anges i punkt 1. Dessa riktlinjer ska utfärdas senast 12 månader efter det att denna förordning har trätt i kraft.

3. För AI-system med hög risk som avses i punkt 5 i bilaga III och som släpps ut på marknaden eller tas i bruk av leverantörer som är finansiella institut som omfattas av krav avseende sina interna styrelseformer, arrangemang eller processer enligt unionslagstiftningen om finansiella tjänster ska underrättelsen om allvarliga incidenter begränsas till dem som avses i artikel 3.44 c.

4. För AI-system med hög risk som utgör säkerhetskomponenter i enheter, eller själva är enheter, omfattade av förordning (EU) 2017/745 och förordning (EU) 2017/746, ska anmälan av allvarliga incidenter begränsas till sådana som avses i artikel 3.44 c och göras till den nationella behöriga myndighet som valts för detta ändamål av de medlemsstater där incidenten inträffade.

KAPITEL 3

VERKSTÄLLIGHET

Artikel 63

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 verkställa denna förordning gäller dock följande:

   a) Alla hänvisningar till en ekonomisk aktör inom ramen för förordning (EU) 2019/1020 ska förstås omfatta alla operatörer som identifieras artikel 2 i den här förordningen.

   b) Alla hänvisningar till en produkt inom ramen för förordning (EU) 2019/1020 ska förstås omfatta 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 rapportera till kommissionen om resultaten av relevant marknadskontroll enligt denna förordning.

3. För AI-system med hög risk som är relaterade till produkter som omfattas av de rättsakter som förtecknas i avsnitt A i bilaga II ska marknadskontrollmyndigheten vid tillämpningen av denna förordning vara den myndighet ansvarig för marknadskontroll som utsetts enligt de rättsakterna eller, under motiverade omständigheter och förutsett att samordning säkerställs, en annan relevant myndighet som fastställts av medlemsstaten.

   De förfaranden som avses i artiklarna 65, 66, 67 och 68 i denna förordning ska inte tillämpas på AI-system som är relaterade till produkter, på vilka de rättsakter som förtecknas i bilaga II avsnitt A är tillämpliga, när sådana rättsakter redan föreskriver förfaranden med samma syfte. I sådana fall ska dessa sektorsspecifika förfaranden tillämpas i stället.

4. För AI-system som släpps ut på marknaden, tas i bruk eller används av finansinstitut som regleras av unionslagstiftningen om finansiella tjänster ska marknadskontrollmyndigheten vid tillämpningen 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.

   Genom undantag från föregående stycke får en annan relevant myndighet, under motiverade omständigheter och under förutsättning att samordning säkerställs, av medlemsstaten identifieras som marknadskontrollmyndighet vid tillämpning av denna förordning.

   Nationella tillsynsmyndigheter som utövar tillsyn av reglerade kreditinstitut som regleras enligt direktiv 2013/36/EU och som deltar i den gemensamma tillsynsmekanism (SSM) som inrättats genom rådets förordning (EU) nr 1204/2013, 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.

5. För AI-system med hög risk som förtecknas i punkt 1 a ska medlemsstaterna, i den mån systemen används för brottsbekämpande ändamål, punkterna 6, 7 och 8 i bilaga III, till marknadskontrollmyndigheter vid tillämpningen av denna förordning utse antingen de nationella myndigheter som utövar tillsyn över brottsbekämpande myndigheter, gränskontrollmyndigheter, immigrationsmyndigheter, asylmyndigheter eller rättsliga myndigheter eller de behöriga tillsynsmyndigheterna för dataskydd enligt direktiv (EU) 2016/680 eller förordning (EU) 2016/679. 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.

6. När unionens institutioner, byråer och organ omfattas av denna förordning ska Europeiska datatillsynsmannen fungera som marknadskontrollmyndighet för dessa.

7. Medlemsstaterna ska underlätta samordningen mellan marknadskontrollmyndigheter som utses enligt denna förordning och andra relevanta nationella myndigheter eller organ som övervakar tillämpningen av den harmoniseringslagstiftning i unionen som förtecknas i bilaga II eller annan unionslagstiftning som kan vara relevant för de AI-system med hög risk som avses i bilaga III.

8. 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 leverantören bevilja dessa fullständig åtkomst till den dokumentation och de tränings-, valideringss- och testningsdataset som används för utvecklingen av AI-systemet 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.

9. Marknadskontrollmyndigheterna ska beviljas tillgång till källkoden för AI-systemet med hög risk på motiverad begäran och endast om följande kumulativa villkor är uppfyllda:

a) Tillgång till källkod är nödvändig för att bedöma om ett AI-system med hög risk uppfyller kraven i avdelning III kapitel 2, och

b) testnings-/revisionsförfaranden och kontroller som grundas på uppgifter och dokumentation från leverantören har uttömts eller visat sig vara otillräckliga.

10. All information och dokumentation som har erhållits av marknadskontrollmyndigheter ska behandlas i enlighet med de konfidentialitetskrav som anges i artikel 70.

11. Klagomål till den berörda marknadskontrollmyndigheten kan lämnas in av varje fysisk eller juridisk person som har skäl att anse att bestämmelserna i denna förordning har överträtts.

I enlighet med artikel 11.3 e och 11.7 a i förordning (EU) 2019/1020 ska klagomål beaktas vid genomförandet av marknadskontrollen och hanteras i enlighet med de särskilda förfaranden som fastställts för detta av marknadskontrollmyndigheterna.

Artikel 63a

Marknadskontrollmyndigheternas tillsyn av testning under verkliga förhållanden

1. Marknadskontrollmyndigheterna ska ha behörighet 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 54, ska marknadskontrollmyndigheterna kontrollera efterlevnaden av bestämmelserna i artikel 54a 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 54a.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 54a och 54b inte är uppfyllda, får den, beroende på vad som är lämpligt, fatta något av följande beslut på sitt territorium:

a) Avbryta eller avsluta testningen under verkliga förhållanden.

b) Kräva att leverantören eller den potentiella leverantören och användaren/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 54a.4 b, ska skälen till beslutet eller invändningen anges i beslutet eller invändningen och formerna och villkoren för att leverantören eller den potentiella leverantören ska kunna bestrida beslutet eller invändningen.

5. I tillämpliga fall ska en marknadskontrollmyndighet, om den har fattat ett beslut som avses i punkt 3 i denna artikel, meddela skälen till detta till marknadskontrollmyndigheterna i de andra medlemsstater där AI-systemet har testats i enlighet med planen för testning.

Artikel 64

Myndigheternas befogenheter att skydda grundläggande rättigheter

1. [utgår]

2. [utgår]

3. Nationella offentliga myndigheter eller organ som utövar tillsyn över eller verkställer 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 när åtkomst till sådan dokumentation är nödvändig för att uppfylla de befogenheter som ingår i myndigheternas eller organens 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.

4. 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 3 och offentliggöra förteckningen. Medlemsstaterna ska anmäla förteckningen till kommissionen och alla andra medlemsstater och ska hålla förteckningen uppdaterad.

5. Om den dokumentation som avses i punkt 3 är otillräcklig för att fastställa huruvida ett åsidosättande av skyldigheter enligt unionsrätt som syftar till att skydda de grundläggande rättigheterna har ägt rum, får den offentliga myndighet eller det offentliga organ som avses i punkt 3 lämna en motiverad begäran till marknadskontrollmyndigheten om att organisera testning av AI-systemet med hög risk genom tekniska medel. Marknadskontrollmyndigheten ska organisera testningen i nära samarbete med den begärande myndigheten eller det begärande organet inom rimlig tid efter begäran.

6. All information och dokumentation som de nationella offentliga myndigheter eller organ som avses i punkt 3 erhåller i enlighet med bestämmelserna i denna artikel ska behandlas i enlighet med de konfidentialitetskrav som fastställs i artikel 70.

Artikel 65

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 det gäller risker för hälsa eller säkerhet eller för personers 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, ska den utvärdera om det berörda AI-systemet uppfyller alla krav och skyldigheter som fastställs i denna förordning. Om risker för de grundläggande rättigheterna identifieras ska marknadskontrollmyndigheten även informera de berörda nationella offentliga myndigheter eller organ som avses i artikel 64.3. De berörda operatörerna ska vid behov samarbeta med marknadskontrollmyndigheterna och andra nationella offentliga myndigheter eller organ som avses i artikel 64.3.

   Om marknadskontrollmyndigheten 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 tid som den fastställer.

   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.

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 av AI-systemet på sin nationella marknad, dra tillbaka produkten från den marknaden eller återkalla den. 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, 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 tillämpningar av artificiell intelligens som avses i artikel 5.

a) AI-systemet med hög risk uppfyller inte kraven i avdelning III kapitel 2.

b) Brister i de harmoniserade standarderna eller gemensamma specifikationerna som avses i artikel 40 och 41 som ger presumtion om överensstämmelse.

c) Bristande efterlevnad av bestämmelserna i artikel 52.

d) AI-systemen för allmänna ändamål uppfyller inte de krav och fullgör inte de skyldigheter som avses i artikel 4a.

7. Marknadskontrollmyndigheterna i andra medlemsstater än den 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 samt eventuella invändningar mot den anmälda nationella åtgärden.

8. Åtgärden ska anses vara berättigad om ingen 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 medlemsstat. Detta påverkar inte den berörda operatörens processuella rättigheter i enlighet med artikel 18 i förordning (EU) 2019/1020. Den period som avses i första meningen i denna punkt ska minskas till 30 dagar vid bristande efterlevnad av förbudet mot de tillämpningar av artificiell intelligens som avses i artikel 5.

9. Marknadskontrollmyndigheterna i alla medlemsstater ska då säkerställa att lämpliga begränsande åtgärder, till exempel att produkten dras tillbaka från marknaden, vidtas i fråga om det berörda AI-systemet utan onödigt dröjsmål.

Artikel 66

Unionsförfarande för skyddsåtgärder

1. Om en medlemsstat inom tre månader efter mottagandet av den anmälan som avses i artikel 65.5, eller inom 30 dagar om det rör sig om bristande efterlevnad av förbudet mot tillämpningar av artificiell intelligens som avses i artikel 5, har gjort invändningar mot en åtgärd som vidtagits av en annan medlemsstat, eller om kommissionen anser att åtgärden strider mot unionsrätten, ska kommissionen utan dröjsmål inleda samråd med den berörda medlemsstatens marknadskontrollmyndighet och operatör eller operatörer och ska utvärdera den nationella åtgärden. På grundval av utvärderingsresultaten ska kommissionen besluta om den nationella åtgärden är berättigad eller inte inom nio månader, eller 60 dagar vid bristande efterlevnad av förbudet mot de tillämpningar av artificiell intelligens som avses i artikel 5, från den anmälan som avses i artikel 65.5. Den ska anmäla detta beslut till den berörda medlemsstaten. Kommissionen ska även informera alla övriga medlemsstater om detta beslut.

2. Om kommissionen anser att den åtgärd som vidtagits av den berörda medlemsstatens marknadskontrollmyndighet är berättigad, ska alla medlemsstaters marknadskontrollmyndigheter säkerställa att lämpliga begränsande åtgärder vidtas med avseende på det berörda AI-systemet, såsom tillbakadragande av AI-systemet från marknaden utan onödigt dröjsmål, och informera kommissionen om detta. Om kommissionen anser att den nationella åtgärden är omotiverad ska marknadskontrollmyndigheten i 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 67

AI-system med hög risk eller för allmänna ändamål som uppfyller kraven och som utgör en risk

1. Om en marknadskontrollmyndighet, efter att ha gjort en utvärdering enligt artikel 65, konstaterar att AI-systemet med hög risk eller för allmänna ändamål uppfyller kraven i denna förordning men ändå utgör en risk för personers hälsa och säkerhet eller för de grundläggande rättigheterna, ska den ålägga den berörda operatören att 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, att dra tillbaka AI-systemet från marknaden eller att återkalla det utan onödigt dröjsmål inom en period som medlemsstaten fastställer.

2. Leverantören eller andra berörda operatörer ska säkerställa att korrigerande åtgärder vidtas i fråga om alla berörda AI-system som de har tillhandahållit på marknaden i unionen inom den tidsfrist som föreskrivs av marknadskontrollmyndigheten i den medlemsstat som avses i punkt 1.

3. Medlemsstaten ska omedelbart informera kommissionen och de andra medlemsstaterna. Den informationen ska innehålla alla tillgängliga 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 de berörda medlemsstaterna och den berörda operatören samt utvärdera den nationella åtgärden. På grundval av utvärderingsresultaten ska kommissionen besluta om åtgärden är berättigad eller inte, och vid behov föreslå lämpliga åtgärder.

5. Kommissionen ska rikta sitt beslut till de berörda medlemsstaterna och informera alla andra medlemsstater.

Artikel 68

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 49.

   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) Identifikationsnumret för det anmälda organ som deltar i förfarandet för bedömning av överensstämmelse har där så är lämpligt inte anbringats.

2. Om den bristande överensstämmelse som avses i punkt 1 kvarstår ska den berörda medlemsstaten vidta alla lämpliga åtgärder för att begränsa eller förbjuda tillhandahållandet av AI-systemet med hög risk på marknaden eller säkerställa att det återkallas eller dras tillbaka från marknaden.

Artikel 68a

Unionsprovningsanläggningar inom artificiell intelligens

1. Kommissionen ska utse en eller flera unionsprovningsanläggningar i enlighet med artikel 21 i förordning (EU) nr 1020/2019 på området artificiell intelligens.

2. Utan att det påverkar verksamheten vid de unionsprovningsanläggningar som avses i artikel 21.6 i förordning (EU) nr 1020/2019 ska de unionsprovningsanläggningar som avses i punkt 1 också tillhandahålla oberoende teknisk eller vetenskaplig rådgivning på begäran av nämnden eller marknadskontrollmyndigheterna.

Artikel 68b

Central pool av oberoende experter

1. På begäran av AI-nämnden ska kommissionen genom en genomförandeakt fastställa bestämmelser om inrättande, underhåll och finansiering av en central pool av oberoende experter för att stödja tillsynsverksamheten enligt denna förordning.

2. Experter ska väljas ut av kommissionen och ingå i den centrala poolen på grundval av aktuell vetenskaplig eller teknisk sakkunskap på området artificiell intelligens, med vederbörlig hänsyn till de tekniska områden som omfattas av kraven och skyldigheterna i denna förordning och marknadskontrollmyndigheternas verksamhet i enlighet med artikel 11 i förordning (EU) nr 1020/2019. Kommissionen ska fastställa antalet experter i poolen utifrån de behov som finns.

3. Experterna får ha följande uppgifter:

a) På begäran av marknadskontrollmyndigheterna ge dessa råd och stödja deras arbete.

b) Stödja gränsöverskridande marknadskontrollsutredningar enligt artikel 58 h, utan att det påverkar marknadskontrollmyndigheternas befogenheter.

c) Ge råd och stöd till kommissionen när den utför sina uppgifter inom ramen för skyddsklausulen enligt artikel 66.

4. Experterna 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. Varje expert ska avge en intresseförklaring, som ska offentliggöras. Kommissionen ska fastställa system och förfaranden för att aktivt hantera och förebygga potentiella intressekonflikter.

5. Medlemsstaterna kan åläggas att betala avgifter för experternas rådgivning och stöd. Strukturen och nivån på avgifterna samt storleken och strukturen på de ersättningsgilla kostnaderna ska antas av kommissionen genom den genomförandeakt som avses i punkt 1, med beaktande av målen för ett korrekt genomförande av denna förordning, kostnadseffektivitet och behovet av att säkerställa att alla medlemsstater har faktisk tillgång till experter.

6. 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 unionsprovningsanläggningarna i enlighet med artikel 68a och experter i enlighet med denna artikel organiseras effektivt och tillför bästa möjliga mervärde.

AVDELNING IX

UPPFÖRANDEKODER

Artikel 69

Uppförandekod för frivillig tillämpning av specifika krav

1. Kommissionen och medlemsstaterna ska underlätta utarbetandet av uppförandekoder som syftar till att uppmuntra frivillig tillämpning av ett eller flera av de krav som anges i avdelning III kapitel 2 i denna förordning på andra AI-system än AI-system med hög risk i största möjliga utsträckning, med beaktande av tillgängliga tekniska lösningar som möjliggör tillämpning av sådana krav.

2. Kommissionen och medlemsstaterna ska underlätta utarbetandet av uppförandekoder som syftar till att uppmuntra frivillig tillämpning på alla AI-system av specifika krav som rör exempelvis miljömässig hållbarhet, inbegripet i fråga om energieffektiv programmering, tillgänglighet för personer med funktionsnedsättning, berörda parters deltagande i utformningen och utvecklingen av AI-systemen och mångfalden i utvecklingsteam på grundval av tydliga mål och centrala resultatindikatorer för att mäta uppnåendet av dessa mål. Kommissionen och medlemsstaterna ska också, när så är lämpligt, underlätta utarbetandet av uppförandekoder som är tillämpliga på frivillig grund med avseende på användarnas skyldigheter när det gäller AI-system.

3. Uppförandekoder som är tillämpliga på frivillig grund får utarbetas av enskilda leverantörer av AI-system eller av organisationer som företräder dem eller av både och, inbegripet genom en involvering av användare och eventuella berörda parter och dessas representativa organisationer eller, om lämpligt, av användare med avseende på deras skyldigheter. Uppförandekoder kan omfatta ett eller flera AI-system med beaktande av likheten mellan de berörda systemens avsedda ändamål.

4. Kommissionen och medlemsstaterna ska när de uppmuntrar och underlättar utarbetandet av uppförandekoder som avses i denna artikel ta hänsyn till de särskilda intressen och behov som små och medelstora företag, inbegripet nystartade företag, har.

AVDELNING X

KONFIDENTIALITET OCH SANKTIONER

Artikel 70

Konfidentialitet

1. Nationella behöriga myndigheter, anmälda organ, kommissionen, nämnden och alla andra fysiska eller juridiska personer som deltar i tillämpningen av denna förordning ska i enlighet med unionsrätten eller nationell rätt vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa 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 direktiv 2016/943 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs.

b) Ett effektivt genomförande av denna förordning, särskilt med avseende på inspektioner, utredningar eller revisioner.

c) Offentliga och nationella säkerhetsintressen.

d) Integriteten i straffrättsliga eller administrativa förfaranden.

e) Integriteten hos information som säkerhetsskyddsklassificerats i enlighet med unionsrätten eller nationell rätt.

2. Utan att det påverkar tillämpningen av punkt 1 ska konfidentiell information som utbyts mellan de nationella behöriga myndigheterna och mellan nationella behöriga myndigheter och kommissionen inte röjas utan föregående samråd med den nationella behöriga myndigheten som informationen härrör från och användaren när sådana AI-system med hög risk som avses i punkterna 1, 6 och 7 i bilaga III används av brottsbekämpande myndigheter, eller gränskontrollmyndigheter, immigrationsmyndigheter eller asylmyndigheter, om ett sådant röjande skulle äventyra allmänna och nationella säkerhetsintressen. Denna skyldighet att utbyta information ska inte omfatta känsliga operativa uppgifter som rör brottsbekämpande myndigheters, gränskontrollmyndigheters samt invandrings- eller asylmyndigheters verksamhet.

Om brottsbekämpande myndigheter eller immigrations- 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 hos dessa myndigheter. Dessa myndigheter ska säkerställa att de marknadskontrollmyndigheter som avses i artikel 63.5 och 63.6, beroende på vad som är tillämpligt, på begäran omedelbart kan få åtkomst till eller få en kopia av denna dokumentation. Endast personal vid marknadskontrollmyndigheten som innehar säkerhetsgodkännande på tillräckligt hög nivå ska ha åtkomst till dokumentationen eller kopior av denna.

3. Punkterna 1 och 2 påverkar inte kommissionens, medlemsstaternas och deras berörda organs samt anmälda organs rättigheter och skyldigheter när det gäller att utbyta information och utfärda varningar, inbegripet i samband med gränsöverskridande samarbete, och inte heller de berörda personernas straffrättsliga skyldighet att lämna information enligt medlemsstaternas rättsordningar.

Artikel 71

Sanktioner

1. Medlemsstaterna ska i enlighet med de villkor som fastställs i denna förordning fastställa regler om sanktioner, inbegripet administrativa sanktionsavgifter, som ska tillämpas vid överträdelser av bestämmelserna i denna förordning och vidta alla nödvändiga åtgärder för att se till att de tillämpas korrekt och effektivt. Sanktionerna ska vara effektiva, proportionella och avskräckande. De ska särskilt ta hänsyn till små och medelstora företags, inbegripet nystartade företags, storlek och intressen och deras ekonomiska bärkraft. De ska också ta hänsyn till huruvida användningen av AI-systemet sker i samband med personlig icke-yrkesmässig verksamhet.

2. Medlemsstaterna ska utan dröjsmål till kommissionen anmäla dessa regler och åtgärder samt eventuella ändringar som berör dem.

3. Bristande efterlevnad av något av förbuden mot tillämpningar av artificiell intelligens enligt artikel 5 ska bli föremål för administrativa sanktionsavgifter på upp till 30 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 6 % av dess totala globala årsomsättning för det föregående räkenskapsåret, beroende på vilket som är högst: När det gäller små och medelstora företag, inbegripet nystartade företag, ska dessa sanktionsavgifter uppgå till högst 3 % av deras globala årsomsättning för det föregående räkenskapsåret.

4. Överträdelser av följande bestämmelser om operatörer eller anmälda organ ska bli föremål för administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 4 % av dess totala globala årsomsättning för det föregående räkenskapsåret, beroende på vilket som är högst::

-a) Leverantörernas skyldigheter enligt artiklarna 4b och 4c.

a) Leverantörernas skyldigheter enligt artikel 16.

b) Skyldigheter för vissa andra personer enligt artikel 23a.

c) Ombudens skyldigheter enligt artikel 25.

d) Importörernas skyldigheter enligt artikel 26.

e) Distributörernas skyldigheter enligt artikel 27.

f) Användarnas skyldigheter enligt artikel 29.1–29.6a.

g) Kraven och skyldigheterna för anmälda organ enligt artiklarna 33, 34.1, 34.3, 34, 34.4 och 34a.

h) Transparensskyldigheterna för leverantörer och användare enligt artikel 52.

När det gäller små och medelstora företag, inbegripet nystartade företag, ska dessa sanktionsavgifter uppgå till högst 2 % av deras globala årsomsättning för det föregående räkenskapsåret.

5. Tillhandahållande av oriktig, ofullständig eller vilseledande information till anmälda organ och nationella behöriga myndigheter som svar på en begäran ska medföra administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 2 % av dess totala globala årsomsättning för det föregående räkenskapsåret, beroende på vilket som är högst. När det gäller små och medelstora företag, inbegripet nystartade företag, ska dessa sanktionsavgifter uppgå till högst 1 % av deras globala årsomsättning för det föregående räkenskapsåret.

6. Vid 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,

aa) om överträdelsen skett med uppsåt eller genom oaktsamhet,

ab) alla åtgärder som vidtagits av operatören för att komma till rätta med överträdelsen och minska dess potentiella negativa effekter,

b) huruvida administrativa sanktionsavgifter redan har tillämpats av andra marknadskontrollmyndigheter i andra medlemsstater på samma operatör för samma överträdelse,

ba) huruvida administrativa sanktionsavgifter redan har tillämpats av andra myndigheter mot 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 rättsakt,

c) storleken på och årsomsättningen och marknadsandelen för den operatör som begått överträdelsen,

d) 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.

7. Varje medlemsstat ska fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och organ som är inrättade i medlemsstaten.

8. Beroende på medlemsstatens rättssystem kan reglerna om administrativa sanktionsavgifter tillämpas på ett sådant sätt att böterna 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.

9. Marknadskontrollmyndighetens utövande av sina befogenheter enligt denna artikel ska omfattas av lämpliga rättssäkerhetsgarantier i enlighet med unionsrätten och medlemsstaternas nationella rätt, inbegripet effektiva rättsmedel och rättssäkerhet.

Artikel 72

Administrativa sanktionsavgifter för unionens institutioner, byråer och organ

1. Europeiska datatillsynsmannen får ålägga böter för de av unionens institutioner, byråer och organ 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,

   b) samarbetet 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, byrå eller organ med avseende på samma fråga,

   c) eventuella liknande tidigare överträdelser som begåtts av unionens institution, byrå eller organ.

2. Bristande efterlevnad av något av de förbud mot tillämpningar av artificiell intelligens som avses i artikel 5 ska medföra administrativa sanktionsavgifter på upp till 500 000 EUR.

3. AI-systemets bristande efterlevnad av andra krav eller skyldigheter enligt denna förordning än de som fastställs i artiklarna 5 och 10 ska medföra administrativa sanktionsavgifter på upp till 250 000 EUR.

4. Innan ett beslut fattas enligt denna artikel ska Europeiska datatillsynsmannen ge unionens institution, byrå eller organ 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 element och omständigheter som de berörda parterna har getts möjlighet att yttra sig om. Eventuella klaganden ska vara nära knutna till förfarandet.

5. De berörda parters 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 deras personuppgifter eller affärshemligheter.

6. De medel som samlats in genom åläggande av avgifter i denna artikel ska utgöra intäkter i unionens allmänna budget.

AVDELNING XI

DELEGERING AV BEFOGENHETER OCH KOMMITTÉFÖRFARANDE

Artikel 73

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den delegering av befogenhet som avses i artiklarna 7.1, 7.3, 11.3, 43.5, 43.6 och 48.5 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 7.1, 7.3, 11.3, 43.5, 43.6 och 48.5 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. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

5. En delegerad akt som antas enligt artiklarna 7.1, 7.3, 11.3, 43.5, 43.6 och 48.5 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 74

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.

AVDELNING XII

SLUTBESTÄMMELSER

Artikel 75

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 åtgärder avseende tekniska specifikationer och förfaranden för godkännande och användning av säkerhetsutrustning som rör AI-system i den mening som avses i Europaparlamentets och rådets förordning (EU) YYY/XX [om artificiell intelligens]*, ska kraven i avdelning III kapitel 2 i den förordningen beaktas.

_____

* Förordning (EU) YYY/XX [om artificiell intelligens] (EUT...).”.

Artikel 76

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 AI-system som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) YYY/XX [om artificiell intelligens]* ska kraven i avdelning III kapitel 2 i den förordningen beaktas.

_____

* Förordning (EU) YYY/XX [om artificiell intelligens] (EUT...).”.

Artikel 77

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 AI-system som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) YYY/XX [om artificiell intelligens]* ska kraven i avdelning III kapitel 2 i den förordningen beaktas.

_____

* Förordning (EU) YYY/XX [om artificiell intelligens] (EUT...).”.

Artikel 78

Ändring av direktiv 2014/90/EU

I artikel 8 i direktiv 2014/90/EU ska följande punkt läggas till:

”4. För AI-system som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) YYY/XX [om artificiell intelligens]* 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.

_____

Förordning (EU) YYY/XX [om artificiell intelligens] (EUT...).”.

Artikel 79

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 AI-system som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) YYY/XX [om artificiell intelligens]* ska kraven i avdelning III kapitel 2 i den förordningen beaktas.

_____

Förordning (EU) YYY/XX [om artificiell intelligens] (EUT...).”.

Artikel 80

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 AI-system som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) YYY/XX [om artificiell intelligens]* ska kraven i avdelning III kapitel 2 i den förordningen beaktas.

_____

Förordning (EU) YYY/XX [om artificiell intelligens] (EUT...).”.

Artikel 81

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 AI-system som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) YYY/XX [om artificiell intelligens]* kraven i avdelning III kapitel 2 i den förordningen beaktas.

_____

* Förordning (EU) YYY/XX [om artificiell intelligens] (EUT...).”.

2. I artikel 19 ska följande punkt läggas till:

”4. Vid antagandet av delegerade akter i enlighet med punkterna 1 och 2 rörande AI-system som är säkerhetskomponenter i den mening som avses i förordning (EU) YYY/XX [om artificiell intelligens] ska kraven som fastställs i avdelning III kapitel 2 i den förordningen beaktas.”.

3. I artikel 43 ska följande punkt läggas till:

”4. Vid antagandet av genomförandeakter i enlighet med punkt 1 rörande AI-system som är säkerhetskomponenter i den mening som avses i förordning (EU) YYY/XX [om artificiell intelligens] ska kraven som fastställs 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 AI-system som är säkerhetskomponenter i den mening som avses i förordning (EU) YYY/XX [om artificiell intelligens] ska kraven som fastställs i avdelning III kapitel 2 i den förordningen beaktas.”.

5. I artikel 57 ska följande punkt läggas till:

”Vid antagandet av de genomförandeakterna rörande AI-system som är säkerhetskomponenter i den mening som avses i förordning (EU) YYY/XX [om artificiell intelligens] ska kraven som fastställs i avdelning III kapitel 2 i den förordningen beaktas.”.

6. I artikel 58 ska följande punkt läggas till:

”3. Vid antagandet av delegerade akter i enlighet med punkterna 1 och 2 rörande AI-system som är säkerhetskomponenter i den mening som avses i förordning (EU) YYY/XX [om artificiell intelligens] ska kraven som fastställs i avdelning III kapitel 2 i den förordningen beaktas.”.

Artikel 82

Ändring av förordning (EU) 2019/2144

I artikel 11 i förordning (EU) 2019/2144 ska följande [punkt/stycke] läggas till:

”3. Vid antagandet av genomförandeakter i enlighet med punkt 2 vad gäller AI-system som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) YYY/XX [om artificiell intelligens]* ska kraven som fastställs i avdelning III kapitel 2 i den förordningen beaktas.

_____

Förordning (EU) YYY/XX [om artificiell intelligens] (EUT...).”.

Artikel 83

AI-system som redan släppts ut på marknaden eller tagits i bruk

1. Denna förordning ska inte tillämpas på AI-system som är komponenter i de stora it-system som inrättats genom de rättsakter som förtecknas i bilaga IX och som har släppts ut på marknaden eller tagits i bruk före den [*12 månader efter den tillämpningsdag för denna förordning som avses i artikel 85.2*], såvida inte dessa rättsakter ersätts eller ändras på ett vis som leder till en betydande ändring av det berörda AI-systemets eller de berörda AI-systemens utformning eller avsedda ändamål.

   De krav som fastställs i denna förordning ska i tillämpliga fall beaktas vid utvärderingen av vart och ett av de stora it-system inrättade genom de rättsakter förtecknade i bilaga IX som ska utföras i enlighet med dessa rättsakter.

2. Denna förordning ska tillämpas på AI-system med hög risk, utom de som avses i punkt 1, som har släppts ut på marknaden eller tagits i bruk före den [*tillämpningsdagen för denna förordning som avses i artikel 85.2*] endast om dessa system från och med den dagen förändras betydligt när det gäller utformning eller avsett ändamål.

Artikel 84

Utvärdering och översyn

1. [utgår]

1b. Kommissionen ska bedöma behovet av att ändra förteckningen i bilaga III var 24:e månad efter det att denna förordning har trätt i kraft och fram till utgången av perioden för delegering av befogenhet. Resultaten av denna bedömning ska läggas fram för Europaparlamentet och rådet.

2. Kommissionen ska senast den [*tre år efter det tillämpningsdatum för denna förordning som avses i artikel 85.2*] och därefter vart fjärde år överlämna en rapport om utvärderingen och översynen av denna förordning till Europaparlamentet och rådet. Rapporten ska offentliggöras.

3. I rapporten som avses i punkt två ska särskild uppmärksamhet ägnas åt

   a) status för de nationella behöriga myndigheternas ekonomiska resurser, tekniska utrustning och personalresurser för att effektivt kunna utföra de uppgifter som de tilldelas enligt denna förordning,

   b) tillståndet för sanktionerna, och särskilt de administrativa sanktionsavgifter som avses i artikel 71.1 som tillämpas av medlemsstaterna på överträdelser av bestämmelserna i denna förordning

4. Senast den [*tre år efter det tillämpningsdatum för denna förordning som avses i artikel 85.2*] och därefter vart fjärde år, i lämpliga fall, ska kommissionen utvärdera den frivilliga uppförandekodernas inverkan och effektivitet för att främja tillämpningen av kraven i avdelning III kapitel 2 för andra AI-system än AI-system med hög risk och eventuellt andra ytterligare krav för AI-system, inbegripet vad gäller miljömässig hållbarhet.

5. Vid tillämpning av punkterna 1a–4 ska nämnden, medlemsstaterna och de nationella behöriga myndigheterna vid begäran tillhandahålla information till kommissionen.

6. Kommissionen ska när den utför de utvärderingar och översyner som avses i punkterna 1a–4 ta hänsyn till ståndpunkter och slutsatser från nämnden, Europaparlamentet, rådet och andra relevanta organ eller källor.

7. Kommissionen ska om nödvändigt överlämna lämpliga förslag om ändring av denna förordning, med särskild hänsyn till teknikens utveckling och mot bakgrund av tendenserna inom informationssamhället.

Artikel 85

Ikraftträdande och tillämpning

1. Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

2. Denna förordning ska tillämpas från och med den [36 månader efter förordningens ikraftträdande].

3. Genom undantag från punkt 2

   a) ska avdelning III kapitel 4 och avdelning VI tillämpas från och med den [tolv månader efter förordningens ikraftträdande],

   b) artikel 71 tillämpas från och med den [tolv månader efter förordningens ikraftträdande].

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

BILAGA I

[utgår]

BILAGA II

FÖRTECKNING ÖVER HARMONISERAD UNIONSLAGSTIFTNING

Avsnitt A - Förteckning över harmoniserad unionslagstiftning 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) [enligt upphävande 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 harmoniserad unionslagstiftning

1. 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).

2. 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).

3. 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).

4. 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).

5. 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).

6. 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).

7. 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).

8. 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, när det gäller obemannade luftfartyg och deras motorer, propellrar, delar och utrustning för kontroll av luftfartyg på distans.

BILAGA III

AI-SYSTEM MED HÖG RISK SOM DET HÄNVISAS TILL I ARTIKEL 6.3

Inom vart och ett av de områden som förtecknas i punkterna 1–8 ska de AI-system som särskilt nämns under varje bokstav anses vara AI-system med hög risk i enlighet med artikel 6.3:

1. Biometri:

   a) System för biometrisk fjärridentifiering.

2. Kritisk infrastruktur:

   (a) AI-system som är avsedda att användas som säkerhetskomponenter i samband med förvaltning och drift av kritisk digital infrastruktur och vägtrafik samt i samband med försörjning av vatten, gas, värme och el.

3. Utbildning och yrkesutbildning:

   (a) AI-system som är avsedda att användas för att fastställa fysiska personers tillgång eller antagande till institutioner eller program för yrkesutbildning eller annan utbildning på alla nivåer.

   (b) AI-system som är avsedda att användas för att utvärdera läranderesultat, när dessa resultat används för att styra fysiska personers inlärningsprocess vid institutioner eller program för yrkesutbildning eller annan utbildning på alla nivåer.

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 som är avsedd att användas för att fatta beslut om befordringar och uppsägningar av arbetsrelaterade avtalsförhållanden, för uppgiftsfördelning på grundval av individuellt beteende eller personlighetsdrag eller egenskaper och för övervakning och utvärdering av anställdas 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 myndigheter eller för offentliga myndigheters räkning för att utvärdera fysiska personers rätt till väsentliga förmåner och tjänster i form av offentligt stöd samt för att bevilja, dra ner på, återkalla eller återkräva 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 tas i bruk av leverantörer som är mikroföretag och små företag enligt definitionen i artikel 3 i bilagan till kommissionens rekommendation 2003/361/EG för deras eget bruk.

(c) AI-system som är avsedda att användas för att sända ut eller för att fastställa prioriteringsordningen för utsändning av larmtjänster, inbegripet brandkår och ambulans.

(d) AI-system som är avsedda att användas för riskbedömning och prissättning i förhållande till fysiska personer när det gäller livförsäkring och sjukförsäkring, med undantag för AI-system som tas i bruk av leverantörer som är mikroföretag och små företag enligt definitionen i bilagan till kommissionens rekommendation 2003/361/EG för deras eget bruk.

6. Brottsbekämpning:

(a) AI-system som är avsedda att användas av brottsbekämpande myndigheter eller på deras vägnar för att bedöma en fysisk persons risk för brott eller återfall eller risken för att en fysisk person blir ett potentiellt brottsoffer.

(b) AI-system som är avsedda att användas av brottsbekämpande myndigheter eller på deras vägnar, såsom lögndetektorer och liknande verktyg, eller för att dra slutsatser om en fysisk persons känslomässiga tillstånd.

(c) [utgår]

(d) AI-system som är avsedda att användas av brottsbekämpande myndigheter eller på deras vägnar för att bedöma hur pass tillförlitlig bevisningen är i samband med utredning eller lagföring av brott.

(e) AI-system som är avsedda att användas av brottsbekämpande myndigheter eller på deras vägnar för att förutsäga att ett faktiskt eller potentiellt brott inträffar eller inträffar på nytt 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 personliga egenskaper eller tidigare brottsliga beteende.

(f) AI-system som är avsedda att användas av brottsbekämpande myndigheter eller på deras vägnar för profilering av fysiska personer enligt artikel 3.4 i direktiv (EU) 2016/680 vid upptäckt, utredning eller lagföring av brott.

(g) [utgår]

7. Migrations-, asyl- och gränskontrollförvaltning:

(a) AI-system som är avsedda att användas av behöriga myndigheter eller på deras vägnar, såsom lögndetektorer och liknande verktyg, eller för att dra slutsatser om en fysisk persons känslomässiga tillstånd.

(b) AI-system som är avsedda att användas av behöriga myndigheter eller på deras vägnar 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) [utgår]

(d) AI-system som är avsedda att användas av behöriga myndigheter eller på deras vägnar för att pröva ansökningar om asyl, visering och uppehållstillstånd och därtill hörande klagomål om huruvida de fysiska personer som ansöker om status är berättigade till stöd.

8. Rättskipning och demokratiska processer:

(a) AI-system som är avsedda att användas av en rättslig myndighet eller på deras vägnar för att tolka fakta eller lagstiftning och att tillämpa lagen på konkreta fakta.

BILAGA IV

TEKNISK DOKUMENTATION enligt 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, den eller de personer som utvecklar systemet, datum för och version av systemet,

   (b) hur AI-systemet interagerar eller kan användas för att interagera med maskinvara eller programvara som inte ingår i själva AI-systemet, i tillämpliga fall,

   (c) versioner av relevant programvara eller inbyggd programvara och eventuella krav med koppling till uppdateringen 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, nedladdningsbart, API osv.),

   (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) bruksanvisning för användaren och, i tillämpliga fall, installationsinstruktioner.

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 förekommande fall, användningen av förtränade system eller verktyg som tillhandahålls av tredje part och hur dessa har använts, integrerats eller ändrats av leverantören,

(b) systemets konstruktionsspecifikationer, dvs. AI-systemets och algoritmernas allmänna logik, de viktigaste konstruktionsvalen, bl.a. den logiska grunden och de antaganden som gjorts, även 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. de beslut om eventuella avvägningar mellan de tekniska lösningarna som valts för att uppfylla kraven i avdelning III kapitel 2,

(c) en beskrivning av systemarkitekturen som förklarar hur programvarukomponenter bygger på eller matas in i varandra och integreras i den övergripande behandlingen, de dataresurser som används för att utveckla, träna, testa och validera AI-systemet,

(d) i tillämpliga 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; informationsklassningsförfaranden (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 användarnas tolkning av AI-systemens resultat, i enlighet med artikel 13.3 d,

(f) i tillämpliga fall, en utförlig beskrivning av förutbestämda ändringar av AI-systemet och dess prestanda, tillsammans med all relevant information om de tekniska lösningar som har valts för att säkerställa att AI-systemet kontinuerligt uppfyller de relevanta kraven i avdelning III kapitel 2,

(g) de validerings- och testförfaranden som används, inklusive information om de validerings- och testdata som har använts och deras huvudsakliga egenskaper; mått som används för att mäta noggrannhet, robusthet, cybersäkerhet och överensstämmelse med andra relevanta krav som anges i avdelning III kapitel 2 samt potentiellt diskriminerande effekter; testloggar och alla testrapporter, daterade och undertecknade av de ansvariga personerna, även med avseende på de förutbestämda ändringar som avses i led f.

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; förutsebara oavsiktliga resultat och källor till risker för hälsa och säkerhet, grundläggande rättigheter och diskriminering med tanke på AI-systemets avsedda syfte; de åtgärder för mänsklig tillsyn som krävs i enlighet med artikel 14, inbegripet de tekniska åtgärder som har vidtagits för att underlätta användarnas tolkning av AI-systemens resultat; specifikationer av indata, beroende på vad som är lämpligt.

4. En utförlig beskrivning av riskhanteringssystemet i enlighet med artikel 9.

5. En beskrivning av relevanta ändringar av systemet som görs av leverantören under dess livscykel.

6. 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 antagits för att uppfylla kraven i avdelning III kapitel 2, inklusive en förteckning över andra relevanta standarder och tekniska specifikationer som har tillämpats.

7. En kopia av EU-försäkran om överensstämmelse.

8. En utförlig beskrivning av det system som har inrättats för att utvärdera AI-systemets prestanda efter det att systemets har släppts ut på marknaden i enlighet med artikel 61, inklusive den plan för övervakning efter utsläppandet på marknaden som avses i artikel 61.3.

BILAGA V

EU-FÖRSÄKRAN OM ÖVERENSSTÄMMELSE

Den EU-försäkran om överensstämmelse som avses i artikel 48 ska innehålla samtliga uppgifter som anges nedan:

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 det berörda AI-systemet överensstämmer med denna förordning och, i tillämpliga fall, med annan relevant unionslagstiftning som föreskriver att en EU-försäkran om överensstämmelse ska utfärdas.

5. Hänvisningar till relevanta harmoniserade standarder som används eller till andra gemensamma specifikationer för vilka överensstämmelse deklareras.

6. I tillämpliga fall, det anmälda organets namn och identifieringsnummer, en beskrivning av det förfarande för bedömning av överensstämmelse som har genomförts och uppgifter om det utfärdade intyget.

7. 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 kvalitetsledningssystemet 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 avdelning III kapitel 2.

4. Leverantören ska också kontrollera att konstruktions- och utvecklingsprocessen för AI-systemet och övervakningen av detta efter utsläppandet på marknaden enligt artikel 61 överensstämmer med den tekniska dokumentationen.

BILAGA VII

BEDÖMNING AV ÖVERENSSTÄMMELSE SOM GRUNDAR SIG PÅ KVALITETSLEDNINGSSYSTEM OCH BEDÖMNING AV DEN TEKNISKA DOKUMENTATIONEN

1. Inledning

Med bedömning av överensstämmelse som grundar sig på kvalitetsledningssystem och bedömning av den tekniska dokumentationen avses det förfarande för bedömning av överensstämmelse som grundar sig på punkterna 2–5.

2. Översikt

Det godkända kvalitetsledningssystemet för konstruktion, 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. Kvalitetsledningssystem

3.1. Leverantörens ansökan ska innehålla följande uppgifter:

(a) Leverantörens namn och adress och, om ansökan lämnas in av ombudet, även dennes namn och adress.

(b) En förteckning över de AI-system som omfattas av samma kvalitetsledningssystem.

(c) Den tekniska dokumentationen för varje AI-system som omfattas av samma kvalitetsledningssystem.

(d) Dokumentation om kvalitetsledningssystemet, som ska omfatta samtliga aspekter som anges i artikel 17.

(e) En beskrivning av de förfaranden som har införts för att säkerställa att kvalitetsledningssystemet förblir lämpligt och effektivt.

(f) En skriftlig försäkran om att samma ansökan inte har lämnats till något annat anmält organ.

3.2. Kvalitetsledningssystemet ska bedömas av det anmälda organet, som ska besluta om det uppfyller kraven i artikel 17.

Beslutet ska meddelas leverantören eller dennes ombud.

Meddelandet ska innehålla slutsatserna från bedömningen av kvalitetsledningssystemet och det motiverade beslutet.

3.3. Det godkända kvalitetsledningssystemet ska fortsätta att användas och underhållas av leverantören så att det förblir lämpligt och effektivt.

3.4. Tillverkaren ska underrätta det anmälda organet om alla planerade ändringar av det godkända kvalitetsledningssystemet 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 kvalitetsledningssystemet 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 beslutet.

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 dokumentation för det AI-system som leverantören avser att släppa ut på marknaden eller ta i bruk och som omfattas av det kvalitetsledningssystem som avses i punkt 3.

4.2. Ansökan ska innehålla följande uppgifter:

(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 testningsdataset som används, inbegripet, när så är lämpligt och med förbehåll för säkerhetsgarantier, genom applikationsprogrammeringsgränssnitt (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 avdelning III kapitel 2. Om det anmälda organet inte nöjer sig med de tester som leverantören har utfört ska det anmälda organet direkt utföra lämpliga tester på lämpligt sätt.

4.5. De anmälda organen ska beviljas tillgång till källkoden för AI-systemet på motiverad begäran och endast om följande kumulativa villkor är uppfyllda:

a) Tillgång till källkod är nödvändig för att bedöma om ett AI-system med hög risk uppfyller kraven i avdelning III kapitel 2.

b) Testnings-/revisionsförfaranden och kontroller som grundas på uppgifter och dokumentation från leverantören har uttömts eller visat sig vara otillräckliga.

4.6. Beslutet ska meddelas leverantören eller dennes ombud. Anmälan ska innehålla slutsatserna från bedömningen av den tekniska dokumentationen och det motiverade beslutet.

Om AI-systemet uppfyller kraven i avdelning III kapitel 2 ska ett EU-intyg 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 avdelning III kapitel 2 ska det anmälda organet vägra att utfärda ett EU-intyg 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 beslutet från det anmälda organ som vägrar att utfärda EU-intyget om 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 godkännas av det anmälda organ som utfärdade EU-intyget 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 EU-intyget 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 EU-intyget om bedömning av teknisk dokumentation, som överlämnas till leverantören.

5. Övervakning av det godkända kvalitetsledningssystemet.

5.1. Syftet med den övervakning som utförs av det anmälda organet och som avses i punkt 3 är att säkerställa att leverantören vederbörligen uppfyller villkoren för det godkända kvalitetsledningssystemet.

5.2. För bedömningsändamål ska leverantören ge det anmälda organet tillträde till de lokaler där konstruktionen, 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 kvalitetsledningssystemet, 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 EU-intyg om bedömning av teknisk dokumentation har utfärdats.

BILAGA VIII UPPGIFTER SOM SKA LÄMNAS IN I SAMBAND MED REGISTRERINGEN AV OPERATÖRER OCH AI-SYSTEM MED HÖG RISK ENLIGT ARTIKEL 51

Leverantörer, ombud och användare som är offentliga myndigheter, byråer eller organ ska lämna den information som avses i del I. Leverantörer eller, i tillämpliga fall, ombud ska säkerställa att den information om deras AI-system med hög risk som avses i punkterna 1–11 i del II är fullständig, korrekt och hålls uppdaterad. Den information som avses i punkt 12 i avsnitt II ska genereras automatiskt av databasen.

Del I. Information om operatörer (vid registrering av operatörer)

-1. Typ av operatör (leverantör, ombud eller användare).

1. Leverantörens namn, adress och kontaktuppgifter.

2. Om uppgifterna lämnas av en annan person för operatörens räkning, dennes namn, adress och kontaktuppgifter.

Del II. Information om AI-systemet med hög risk

1. Leverantörens namn, adress och kontaktuppgifter.

2. Namn, adress och kontaktuppgifter för tillverkarens ombud, i förekommande fall.

3. AI-systemets handelsnamn och eventuella ytterligare entydiga hänvisningar som gör det möjligt att identifiera och spåra AI-systemet.

4. Beskrivning av AI-systemets avsedda syfte.

5. AI-systemets status (på marknaden eller i bruk; finns inte längre på marknaden/i bruk, har återkallats).

6. Typ, nummer och sista giltighetsdag för det intyg som utfärdats av det anmälda organet samt det anmälda organets namn eller identifikationsnummer, i tillämpliga fall.

7. En skannad kopia av det intyg som avses i punkt 6, i tillämpliga fall.

8. Medlemsstater där AI-systemet släpps ut eller har släppts ut på marknaden, tagits i bruk eller gjorts tillgängligt i unionen.

9. En kopia av den EU-försäkran om överensstämmelse som avses i artikel 48.

10. Elektroniska bruksanvisningar.

11. URL för ytterligare information (valfritt).

12. Användarnas namn, adress och kontaktuppgifter.

BILAGA VIIIa

INFORMATION SOM SKA LÄMNAS VID REGISTRERING AV AI-SYSTEM AV HÖG RISK SOM FÖRTECKNAS I BILAGA III I SAMBAND MED TESTNING UNDER VERKLIGA FÖRHÅLLANDEN I ENLIGHET MED ARTIKEL 54a

Följande uppgifter ska lämnas och därefter hållas uppdaterade när det gäller testning under verkliga förhållanden som ska registreras i enlighet med artikel 54a.

1. Det enda unionsomfattande identifikationsnumret för testningen under verkliga förhållanden.

2. Namn och kontaktuppgifter för den leverantör eller potentiella leverantör och för användare 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 avbrott eller avslutande av testningen under verkliga förhållanden.

BILAGA IX

Unionslagstiftning om stora it-system på området 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) Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om ändring av förordning (EG) nr 767/2008, förordning (EG) nr 810/2009, förordning (EU) 2017/2226, förordning (EU) 2016/399, förordning XX/2018 [förordning om interoperabilitet] och beslut 2004/512/EG och om upphävande av rådets beslut 2008/633/RIF (COM(2018) 302 final). Kommer att uppdateras när förordningen har antagits (april/maj 2021) av medlagstiftarna.

3. Eurodac

(a) Ändrat förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om inrättande av Eurodac för jämförelse av biometriska uppgifter för en effektiv tillämpning av förordning (EU) XXX/XXX [förordningen om asyl- och migrationshantering] och förordning (EU) XXX/XXX [vidarebosättningsförordningen], 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/EEG (COM(2020) 614 final).

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. Driftskompatibilitet

(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).