EUROPEISKA
KOMMISSIONEN

Bryssel den 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

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

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

1.1. Motiv och syfte med förslaget

Denna motivering åtföljer förslaget till förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens). Artificiell intelligens (AI) tillhör en teknikfamilj under snabb utveckling som kan ge en mängd ekonomiska och samhälleliga vinster över hela spektrumet av näringslivssektorer och samhällsverksamheter. Genom att ge bättre prognoser, optimera verksamhet och resurstilldelning samt individanpassa tillhandahållandet av tjänster kan användningen av artificiell intelligens stödja socialt och miljömässigt fördelaktiga resultat och ge viktiga konkurrensfördelar för företagen och den europeiska ekonomin. Sådana åtgärder behövs särskilt inom sektorer med stor genomslagskraft, bland annat klimatförändring, miljö och hälsa, den offentliga sektorn, finanser, rörlighet, inrikes frågor och jordbruk. Men samma faktorer och teknik som driver de socioekonomiska fördelarna med AI kan också leda till nya risker eller negativa konsekvenser för enskilda personer eller samhället som helhet. Mot bakgrund av den snabba tekniska utvecklingen och eventuella utmaningar har EU åtagit sig att eftersträva en balanserad strategi. Det ligger i unionens intresse att bevara EU:s tekniska ledarskap och se till att européerna kan dra nytta av ny teknik som utvecklas och fungerar i enlighet med unionens värden, grundläggande rättigheter och principer.

Detta förslag uppfyller det politiska åtagandet från ordförande Ursula von der Leyen, som i sina politiska riktlinjer för kommissionen 2019–2024 *En ambitiösare union*[1] tillkännagav att kommissionen skulle lägga fram lagstiftning för en samordnad europeisk strategi om de mänskliga och etiska konsekvenserna av AI. Efter detta tillkännagivande offentliggjorde kommissionen den 19 februari 2020 vitboken om AI – En europeisk strategi för spetskompetens och förtroende[2]. I vitboken anges politiska alternativ för hur man ska uppnå det dubbla målet att främja spridningen av AI och hantera de risker som är förknippade med viss användning av sådan teknik. Syftet med detta förslag är att genomföra det andra målet och utveckla av ett ekosystem av förtroende genom att föreslå en rättslig ram för tillförlitlig AI. Förslaget bygger på EU:s värden och grundläggande rättigheter och syftar till att se till att människor och andra användare kan känna sig trygga att anamma AI-baserade lösningar och samtidigt uppmuntra företagen att utveckla dem. AI bör vara ett verktyg för människor och vara en positiv kraft i samhället med det yttersta målet att öka människors välbefinnande. Reglerna för sådan AI som är tillgänglig på unionsmarknaden eller som på annat sätt påverkar människor i unionen bör därför vara människocentrerade, så att människor kan lita på att tekniken används på ett sätt som är säkert och förenligt med lagstiftningen, inbegripet respekten för de grundläggande rättigheterna. Efter offentliggörandet av vitboken inledde kommissionen ett brett samråd med berörda parter, som möttes med stort intresse av ett stort antal berörda parter som till stor del stödde lagstiftningsåtgärder för att hantera de utmaningar och farhågor som den ökade användningen av AI ger upphov till.

Förslaget är också ett svar på uttryckliga krav från Europaparlamentet och Europeiska rådet, som upprepade gånger har uttryckt krav på lagstiftningsåtgärder för att säkerställa en välfungerande inre marknad för system med artificiell intelligens (*AI-system*) där både fördelar och risker med AI hanteras på lämpligt sätt på unionsnivå. Förslaget stöder unionens

[1] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

[2] Europeiska kommissionen, vitbok om artificiell intelligens – En europeisk strategi för spetskompetens och förtroende (COM(2020) 65 final, 2020).

mål att bli världsledande inom utvecklingen av säker, tillförlitlig och etisk artificiell intelligens, såsom fastställts av Europeiska rådet[3], och säkerställer skyddet av etiska principer, såsom särskilt begärts av Europaparlamentet[4].

År 2017 efterlyste Europeiska rådet en ”handlingsberedskap när det gäller att reagera på nya utvecklingstrender”, inbegripet ”frågor som artificiell intelligens /.../ med samtidigt säkerställande av dataskydd, digitala rättigheter och etiska normer på hög nivå”[5]. I sina slutsatser från 2019 om den samordnade planen för utveckling och användning av europeisk artificiell intelligens[6] betonade rådet ytterligare vikten av att säkerställa att EU-medborgarnas rättigheter respekteras fullt ut och efterlyste en översyn av befintlig relevant lagstiftning för att göra den ändamålsenlig för de nya möjligheter och utmaningar som AI ger upphov till. Europeiska rådet har också efterlyst att det tydligt fastställs vilka AI-tillämpningar som bör betraktas ha hög risk[7].

I de senaste slutsatserna av den 21 oktober 2020 efterlystes ytterligare åtgärder mot bristande insyn, komplexitet, snedvridenhet, en viss grad av oförutsägbarhet och delvis autonomt beteende hos vissa AI-system, för att säkerställa att systemen är förenliga med grundläggande rättigheter och underlätta genomförandet av rättsregler[8].

Europaparlamentet har också utfört betydande arbete på AI-området. I oktober 2020 antog parlamentet ett antal resolutioner om AI, bland annat om etik[9], skadestånd[10] och upphovsrätt[11]. Under 2021 följdes dessa av resolutioner om AI i straffrättsliga frågor[12] och inom utbildning, kultur och den audiovisuella sektorn[13]. I Europaparlamentets resolution om en ram för etiska aspekter av artificiell intelligens, robotteknik och tillhörande teknik rekommenderas särskilt kommissionen att föreslå lagstiftningsåtgärder för att utnyttja möjligheterna och fördelarna med AI, men också att säkerställa skydd av etiska principer. Resolutionen innehåller texten till ett förslag till förordning om etiska principer för utveckling, införande och användning av AI, robotteknik och tillhörande teknik. I enlighet med det politiska åtagande som kommissionens ordförande Ursula von der Leyen gjorde i sina politiska riktlinjer när det gäller resolutioner som Europaparlamentet antagit i enlighet

---

3 Europeiska rådet, Extra möte i Europeiska rådet (1 och 2 oktober 2020) – Slutsatser, EUCO 13/20, 2020, s. 6.

4 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)).

5 Europeiska rådet, *Europeiska rådets möte (den 19 oktober 2017) – Slutsats* EUCO 14/17, 2017, s. 8.

6 Europeiska unionens råd, *Artificiell intelligens b) Slutsatser om den samordnade planen för artificiell intelligens – Antagande* 6177/19, 2019.

7 Europeiska rådet, *Extra möte i Europeiska rådet (1 och 2 oktober 2020) – Slutsatser* EUCO 13/20, 2020.

8 Europeiska unionens råd, *Ordförandeskapets slutsatser – Stadgan om de grundläggande rättigheterna i fråga om artificiell intelligens och digitalisering*, 11481/20, 2020.

9 Europaparlamentets resolution av den 20 oktober 2020 om en ram för etiska aspekter av artificiell intelligens, robotteknik och tillhörande teknik (2020/2012(INL)).

10 Europaparlamentets resolution av den 20 oktober 2020 om en skadeståndsordning för artificiell intelligens (2020/2014 (INL)).

11 Europaparlamentets resolution av den 20 oktober 2020 om immateriella rättigheter för utveckling av artificiell intelligens (2020/2015(INI)).

12 Europaparlamentets förslag till betänkande om artificiell intelligens inom straffrätten och polisens och rättsväsendets användning av artificiell intelligens i brottmål (2020/2016(INI)).

13 Europaparlamentets förslag till betänkande om artificiell intelligens inom utbildning, kultur och den audiovisuella sektorn (2020/2017(INI)). Kommissionen har därför antagit handlingsplanen för digital utbildning 2021–2027: Ställa om utbildningen till den digitala tidsåldern, som förutser utarbetandet av etiska riktlinjer för AI och dataanvändning inom utbildningen – kommissionens meddelande (COM(2020) 624 final).

med artikel 225 i fördraget om Europeiska unionens funktionssätt (*EUF-fördraget*), beaktar detta förslag Europaparlamentets ovannämnda resolution med full respekt för principerna om proportionalitet, subsidiaritet och bättre lagstiftning.

Mot denna politiska bakgrund lägger kommissionen fram det föreslagna regelverket för artificiell intelligens med följande **specifika mål**:

- Säkerställa att AI-system som släpps ut och används på unionsmarknaden är säkra och är förenliga med befintlig lagstiftning om de grundläggande rättigheterna och unionens värden.
- Säkerställa rättssäkerhet för att underlätta investeringar och innovation för AI.
- Förbättra styrningen och säkra en effektiv kontroll av uppfyllandet av befintlig lagstiftning om de grundläggande rättigheterna och säkerhetskrav som är tillämpliga på AI-system.
- Främja utvecklingen av en inre marknad för lagliga, säkra och tillförlitliga AI-tillämpningar och förhindra marknadsfragmentering.

För att uppnå dessa mål presenteras i detta förslag en balanserad och proportionerlig övergripande regleringsstrategi för AI som begränsar sig till de minimikrav som är nödvändiga för att hantera de risker och problem som är förknippade med AI, utan att i onödan eller på ett oproportionerligt sätt begränsa eller hindra den tekniska utvecklingen eller på annat sätt öka kostnaderna för att släppa ut AI-lösningar på marknaden. I förslaget fastställs en stabil och flexibel rättslig ram. Dels är den heltäckande och framtidssäkrad i dess grundläggande regleringsval, inbegripet de principbaserade krav som AI-systemen bör uppfylla. Dels införs ett proportionerligt regelverk som är inriktat på en väldefinierad riskbaserad regleringsmetod som inte skapar onödiga handelshinder, varigenom rättsliga ingripanden skräddarsys för de konkreta situationer där det finns berättigade skäl till farhågor eller där sådana farhågor rimligen kan förutses inom en nära framtid. Samtidigt innehåller den rättsliga ramen flexibla mekanismer som gör det möjligt att anpassa den dynamiskt allteftersom tekniken utvecklas och nya farhågor dyker upp.

I förslaget fastställs harmoniserade regler för utveckling, utsläppande på marknaden och användning av AI-system i unionen enligt en proportionerlig riskbaserad metod. I det föreslås en enda framtidssäkrad definition av AI. Vissa särskilt skadliga AI-metoder är förbjudna eftersom de strider mot unionens värden, medan särskilda begränsningar och skyddsåtgärder föreslås i samband med viss användning av biometriska fjärridentifieringssystem för brottsbekämpande ändamål. I förslaget fastställs en solid riskmetod för att definiera AI-system med ”hög risk”, som medför betydande risker för människors hälsa och säkerhet eller grundläggande rättigheter. Dessa AI-system måste uppfylla en uppsättning övergripande obligatoriska krav på tillförlitlig AI och genomgå förfaranden för bedömning av överensstämmelse innan de kan släppas ut på unionsmarknaden. Leverantörer och användare av dessa system åläggs också förutsägbara, proportionella och tydliga skyldigheter för att säkerställa säkerhet och iakttagande av befintlig lagstiftning som skyddar de grundläggande rättigheterna under hela AI-systemens livscykel. För vissa specifika AI-system föreslås endast minimikrav på transparens, särskilt när chatbotar eller ”deepfake” används.

De föreslagna reglerna kommer att verkställas genom ett styrningssystem på medlemsstatsnivå, som bygger på redan befintliga strukturer, och en samarbetsmekanism på unionsnivå genom inrättandet av en europeisk nämnd för artificiell intelligens. Ytterligare åtgärder föreslås också för att stödja innovation, särskilt genom ”regulatoriska sandlådor” för AI och andra åtgärder för att minska regelbördan och stödja små och medelstora företag samt nystartade företag.

1.2. Förenlighet med befintliga bestämmelser inom området

Förslagets övergripande karaktär kräver full överensstämmelse med den befintliga unionslagstiftning som är tillämplig på de sektorer där AI-system med hög risk redan används eller sannolikt kommer att användas inom en nära framtid.

Överensstämmelse säkerställs också med EU-stadgan om de grundläggande rättigheterna och unionens befintliga sekundärlagstiftning om dataskydd, konsumentskydd, icke-diskriminering och jämställdhet. Förslaget påverkar inte – utan kompletterar – den allmänna dataskyddsförordningen (förordning (EU) 2016/679) och brottsbekämpningsdirektivet (direktiv (EU) 2016/680) med en uppsättning harmoniserade regler för utformning, utveckling och användning av vissa AI-system med hög risk och begränsningar för viss användning av biometriska fjärridentifieringssystem. Dessutom kompletterar förslaget befintlig unionslagstiftning om icke-diskriminering med särskilda krav som syftar till att minimera risken för algoritmisk diskriminering, särskilt när det gäller utformningen av och kvaliteten på de dataset som används för utveckling av AI-system, kompletterat med skyldigheter avseende testning, riskhantering, dokumentation och mänsklig tillsyn under AI-systemens hela livscykel. Förslaget påverkar inte tillämpningen av unionens konkurrenslagstiftning.

För AI-system med hög risk som utgör säkerhetskomponenter i produkter kommer detta förslag att integreras i befintlig sektorsspecifik säkerhetslagstiftning för att säkerställa enhetlighet, motverka dubbelarbete och minimera ytterligare bördor. Särskilt när det gäller AI-system med hög risk i samband med produkter som omfattas av lagstiftning som ingår i den nya lagstiftningsramen (t.ex. maskiner, medicintekniska produkter, leksaker) kommer de krav på AI-system som fastställs i detta förslag att kontrolleras som en del av de befintliga förfarandena för bedömning av överensstämmelse enligt relevant lagstiftning i den nya lagstiftningsramen. När det gäller samspelet mellan kraven är avsikten att de säkerhetsrisker som är specifika för AI-system ska omfattas av kraven i detta förslag, medan lagstiftningen i den nya lagstiftningsramen syftar till att säkerställa slutproduktens övergripande säkerhet och därför kan innehålla särskilda krav på säker integrering av ett AI-system i slutprodukten. Förslaget till maskinförordning, som antas samma dag som detta förslag, återspeglar detta tillvägagångssätt fullt ut. Detta förslag skulle inte vara direkt tillämpligt för AI-system med hög risk när det gäller produkter som omfattas av relevant lagstiftning enligt den gamla metoden (t.ex. luftfart, bilar). De grundläggande förhandskrav för AI-system med hög risk som fastställs i detta förslag måste dock beaktas när relevant genomförandelagstiftning eller delegerad lagstiftning antas enligt dessa akter.

När det gäller AI-system som tillhandahålls eller används av reglerade kreditinstitut bör de myndigheter som ansvarar för tillsynen av unionens lagstiftning om finansiella tjänster utses till behöriga myndigheter för tillsyn av kraven i detta förslag, för att säkerställa en enhetlig efterlevnad av skyldigheterna enligt detta förslag och unionens lagstiftning om finansiella tjänster, där AI-system till viss del regleras indirekt i samband med kreditinstitutens interna styrningssystem. För att ytterligare öka enhetligheten integreras förfarandet för bedömning av överensstämmelse och vissa av leverantörernas förfarandeskyldigheter enligt detta förslag i förfarandena enligt direktiv 2013/36/EU om behörighet att utöva verksamhet i kreditinstitut och om tillsyn[14].

[14] 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 (Text av betydelse för EES) (EUT L 176, 27.6.2013, s. 338).

Detta förslag är också förenligt med tillämplig unionslagstiftning om tjänster, bland annat om förmedlingstjänster som regleras genom direktiv 2000/31/EG om elektronisk handel[15] och kommissionens nyligen framlagda förslag till rättsakt om digitala tjänster[16].

När det gäller AI-system som är komponenter i stora it-system inom området med frihet, säkerhet och rättvisa som förvaltas av Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (*eu-LISA*) kommer förslaget inte att tillämpas på de AI-system som har släppts ut på marknaden eller tagits i bruk innan ett år har förflutit från den dag då denna förordning börjar tillämpas, såvida inte en ersättning eller ändring av dessa rättsakter leder till en betydande förändring av det berörda AI-systemets eller de berörda AI-systemens utformning eller avsedda ändamål.

1.3. Förenlighet med unionens politik inom andra områden

Förslaget ingår i ett bredare omfattande åtgärdspaket som hanterar de problem som utvecklingen och användningen av AI ger upphov till, i enlighet med vitboken om AI. Förenlighet och komplementaritet säkerställs därför med andra pågående eller planerade kommissionsinitiativ som också syftar till att hantera dessa problem, inbegripet översynen av sektorspecifik produktlagstiftning (t.ex. maskindirektivet och direktivet om allmän produktsäkerhet) och initiativ som tar upp ansvarsfrågor i samband med ny teknik, inbegripet AI-system. Dessa initiativ kommer att bygga vidare på och komplettera detta förslag för att skapa rättslig klarhet och främja utvecklingen av ett ekosystem av förtroende för AI i Europa.

Förslaget är också förenligt med kommissionens övergripande digitala strategi i och med att det ska bidra till att främja en teknik för människor, en av de tre huvudpelarna i den politiska inriktning och de mål som tillkännagavs i meddelandet *Att forma EU:s digitala framtid*[17]. Där fastställs en enhetlig, effektiv och proportionerlig ram för att se till att AI utvecklas på ett sätt som respekterar människors rättigheter och vinner deras förtroende, gör Europa rustat för den digitala tidsåldern och omvandlar de kommande tio åren till det **digitala decenniet**[18].

Främjandet av AI-driven innovation är dessutom nära kopplat till **dataförvaltningsakten**[19], **direktivet om öppna data**[20] och andra initiativ inom ramen för **EU:s datastrategi**[21], som kommer att inrätta betrodda mekanismer och tjänster för vidareutnyttjande, delning och sammanslagning av data som är avgörande för utvecklingen av datadrivna AI-modeller av hög kvalitet.

Förslaget stärker också avsevärt unionens roll när det gäller att bidra till utformningen av globala normer och standarder samt främja tillförlitlig AI som är förenlig med unionens värderingar och intressen. Det ger unionen en stark grund för att fördjupa samarbetet om frågor som rör AI med sina externa partner, inbegripet tredjeländer, och i internationella forum.

---

15 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).

16 Se förslaget till Europaparlamentets och rådets förordning om en inre marknad för digitala tjänster (rättsakten om digitala tjänster) och om ändring av direktiv 2000/31/EG (COM(2020) 825 final).

17 Meddelande från kommissionen, Att forma EU:s digitala framtid (COM/2020/67 final).

18 Den digitala kompassen 2030: den europeiska vägen för det digitala decenniet.

19 Förslag till förordning om dataförvaltning (dataförvaltningsakten) COM/2020/767.

20 Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn (PE/28/2019/REV/1) (EUT L 172, 26.6.2019, s. 56).

21 Kommissionens meddelande En europeisk strategi för data (COM/2020/66 final).

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

2.1. Rättslig grund

Den rättsliga grunden för förslaget är i första hand artikel 114 i EUF-fördraget, där det föreskrivs att det ska beslutas om åtgärder för att säkerställa upprättandet av den inre marknaden och dess funktion.

Detta förslag utgör en central del av EU:s strategi för den digitala inre marknaden. Det främsta syftet med förslaget är att säkerställa en väl fungerande inre marknad genom att fastställa harmoniserade regler särskilt om utveckling, utsläppande på unionsmarknaden och användning av produkter och tjänster som utnyttjar AI-teknik eller tillhandahålls som fristående AI-system. Vissa medlemsstater överväger redan nationella regler för att säkerställa att AI är säker och att den utvecklas och används i enlighet med skyldigheter som rör grundläggande rättigheter. Detta kommer sannolikt att leda till två stora problem: i) en fragmentering av den inre marknaden när det gäller väsentliga delar, särskilt när det gäller kraven för AI-produkter och AI-tjänster, deras marknadsföring, deras användning, de offentliga myndigheternas ansvar och tillsyn samt ii) en väsentlig försämring av rättssäkerheten för både leverantörer och användare av AI-system om hur befintliga och nya regler kommer att tillämpas på dessa system i unionen. Med tanke på den stora spridningen av produkter och tjänster över gränserna kan dessa två problem bäst lösas genom en harmoniserad EU-lagstiftning.

I förslaget fastställs mycket riktigt gemensamma obligatoriska krav som är tillämpliga på utformning och utveckling av vissa AI-system innan de släpps ut på marknaden och som kommer att ytterligare konkretiseras genom harmoniserade tekniska standarder. Förslaget tar också upp situationen efter att AI-system har släppts ut på marknaden genom att harmonisera det sätt på vilket efterhandskontroller utförs.

Eftersom detta förslag dessutom innehåller vissa särskilda regler för skydd av individer när det gäller behandling av personuppgifter, särskilt begränsningar av användningen 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.

2.2. Subsidiaritetsprincipen (för icke-exklusiv befogenhet)

AI:s natur, som ofta bygger på stora och varierande dataset och som kan ingå i en produkt eller tjänst som cirkulerar fritt på den inre marknaden, innebär att målen för detta förslag inte kan uppnås på ett effektivt sätt av medlemsstaterna på egen hand. Dessutom kommer ett framväxande lapptäcke av potentiellt avvikande nationella regler att hindra en smidig rörlighet av produkter och tjänster som rör AI-system över hela EU och kommer att vara ineffektivt när det gäller att säkerställa säkerheten och skyddet av de grundläggande rättigheterna och unionens värden i de olika medlemsstaterna. Nationella strategier för att hantera problemen kommer endast att skapa ytterligare rättslig osäkerhet och hinder, och kommer att leda till långsammare spridning på marknaden av AI.

Målen för detta förslag kan bättre uppnås på unionsnivå, så att en ytterligare fragmentering av den inre marknaden i potentiellt motstridiga nationella ramar som förhindrar en fri rörlighet av varor och tjänster i vilka AI ingår undviks. Ett stabilt europeiskt regelverk för tillförlitlig AI kommer också att säkerställa lika villkor och skydda alla människor, samtidigt som Europas konkurrenskraft och industriella bas inom AI stärks. Endast gemensamma åtgärder på unionsnivå kan också skydda unionens digitala suveränitet och utnyttja dess verktyg och regleringsmakt för att utforma globala regler och standarder.

2.3. Proportionalitetsprincipen

Förslaget bygger på befintliga rättsliga ramar och är proportionerligt och nödvändigt för att uppnå målen, eftersom det följer en riskbaserad metod och medför regelbördor endast när AI-system sannolikt medför stora risker för de grundläggande rättigheterna och säkerheten. För andra AI-system, som inte utgör hög risk, införs endast mycket begränsade transparenskrav, till exempel när det gäller tillhandahållande av information för att flagga att ett AI-system används vid interaktion med människor. När det gäller AI-system med hög risk är kraven på högkvalitativa data, dokumentation och spårbarhet, transparens, mänsklig tillsyn, noggrannhet och robusthet absolut nödvändiga för att minska de risker för de grundläggande rättigheterna och säkerheten som AI utgör och som inte omfattas av andra befintliga rättsliga ramar. Harmoniserade standarder och stödverktyg för vägledning och efterlevnad kommer att hjälpa leverantörer och användare att uppfylla de krav som fastställs i förslaget och minimera kostnaderna för dem. Aktörernas kostnader står i proportion till de mål som uppnås och till de ekonomiska fördelar och det förbättrade anseende som aktörerna kan förvänta sig av detta förslag.

2.4. Val av instrument

Valet av en förordning som rättsligt instrument motiveras av behovet av enhetlig tillämpning av de nya reglerna, såsom definitionen av AI, förbudet mot vissa skadliga AI-baserade metoder och klassificeringen av vissa AI-system. En förordnings direkta tillämplighet i enlighet med artikel 288 i EUF-fördraget kommer att minska den rättsliga fragmenteringen och underlätta utvecklingen av en inre marknad för lagliga, säkra och tillförlitliga AI-system. Den kommer särskilt att göra detta genom att introducera en harmoniserad uppsättning grundläggande krav för AI-system som klassificeras ha hög risk och skyldigheter för leverantörer och användare av dessa system, förbättra skyddet av de grundläggande rättigheterna och skapa rättssäkerhet för både operatörer och konsumenter.

Samtidigt är bestämmelserna i förordningen inte alltför detaljerade och lämnar utrymme för olika nivåer av åtgärder från medlemsstaternas sida för element som inte undergräver initiativets mål, särskilt den interna organisationen av marknadskontrollsystemet och införandet av åtgärder för att främja innovation.

3. RESULTAT AV EFTERHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

3.1. Samråd med berörda parter

Detta förslag är resultatet av ett omfattande samråd med alla viktiga berörda parter, där de allmänna principerna och miniminormerna för kommissionens samråd med berörda parter tillämpades.

Ett **offentligt samråd på nätet** inleddes den 19 februari 2020 i samband med offentliggörandet av vitboken om artificiell intelligens och pågick till och med den 14 juni 2020. Syftet med samrådet var att samla in synpunkter och åsikter om vitboken. Den riktade sig till alla intresserade berörda parter från den offentliga och privata sektorn, däribland regeringar, lokala myndigheter, kommersiella och icke-kommersiella organisationer, arbetsmarknadsparter, experter, akademiker och medborgare. Efter analys av alla mottagna svar offentliggjorde kommissionen både en sammanfattning och de enskilda svaren på sin webbplats[22].

[22] Se alla resultaten från samrådet här.

Totalt inkom 1 215 bidrag, varav 352 kom från företag, företagarorganisationer eller näringslivsorganisationer, 406 från enskilda personer (92 % från EU), 152 från akademiska institutioner och forskningsinstitut och 73 från offentliga myndigheter. Det civila samhället företräddes av 160 svarande (varav 9 var konsumentorganisationer, 129 icke-statliga organisationer och 22 fackföreningar) och 72 svarande klassificerade sig som ”övriga”. Av de 352 företags- och industriföreträdarna var 222 företag och företrädare för näringslivet, varav 41,5 % var mikroföretag eller små och medelstora företag. De övriga var näringslivsorganisationer. Totalt kom 84 % av svaren från näringslivet och industrin från EU-27. Beroende på frågan använde 81–598 av de svarande möjligheten att lägga till fritextkommentarer. Över 450 ståndpunktsdokument lämnades in via webbplatsen EU Survey, antingen som komplement till svaren på frågeformuläret (över 400) eller som fristående bidrag (över 50).

På det hela taget råder det en allmän enighet bland berörda parter om att det behövs åtgärder. En stor majoritet av de berörda parterna är överens om att det finns luckor i lagstiftningen eller att ny lagstiftning behövs. Flera berörda parter varnar dock att kommissionen ska motverka dubbelarbete samt undvika motstridiga skyldigheter och överreglering. I många kommentarer underströks vikten av ett teknikneutralt och proportionerligt regelverk.

De berörda parterna begärde oftast en snäv, tydlig och exakt definition av AI. Berörda parter betonade också att det förutom förtydligandet av termen AI är viktigt att definiera termerna ”risk”, ”hög risk”, ”låg risk”, ”biometrisk fjärridentifiering” och ”skada”.

De flesta av de svarande förhåller sig uttryckligen positivt till den riskbaserade metoden. Att använda en riskbaserad ram ansågs vara ett bättre alternativ än en heltäckande reglering av alla AI-system. De olika typerna av risker och hot bör bedömas sektorsvis och från fall till fall. Vid beräkningen av riskerna bör också konsekvenserna för rättigheterna och säkerheten beaktas.

Regulatoriska sandlådor skulle kunna vara mycket användbara för främjandet av AI och välkomnas av vissa berörda parter, särskilt näringslivsorganisationerna.

Bland dem som yttrade sig om genomförandemodellerna var mer än 50 %, särskilt från näringslivsorganisationerna, positiva till en kombination av en självriskbedömning på förhand och en efterhandskontroll av AI-system med hög risk.

3.2. Insamling och användning av sakkunnigutlåtanden

Förslaget bygger på två års analys och ett nära samarbete med berörda parter, däribland akademiker, företag, arbetsmarknadens parter, icke-statliga organisationer, medlemsstater och medborgare. Det förberedande arbetet inleddes 2018 i och med inrättandet av en **högnivåexpertgrupp för artificiell intelligens** (*AI-expertgruppen*) med en inkluderande och bred sammansättning på 52 välkända experter som hade i uppgift att ge kommissionen råd om genomförandet av kommissionens strategi för artificiell intelligens. I april 2019 gav kommissionen sitt stöd[23] till de centrala kraven i AI-expertgruppens etiska riktlinjer för tillförlitlig AI[24], som hade reviderats för att ta hänsyn till mer än 500 bidrag från berörda parter. Nyckelkraven återspeglar en bred och gemensam syn, vilket framgår av en mängd etiska koder och principer som tagits fram av många privata och offentliga organisationer i och utanför Europa, om att utveckling och användning av AI bör styras av vissa

[23] Europeiska kommissionen, *Att skapa förtroende för människocentrerad artificiell intelligens* (COM(2019) 168).

[24] AI-expertgruppen, *Etiska riktlinjer för tillförlitlig AI*, 2019.

grundläggande värdeorienterade principer. Genom bedömningslistan för tillförlitlig artificiell intelligens[25] började dessa krav gälla i en pilotprocess med över 350 organisationer.

Dessutom bildades **AI-alliansen**[26] som en plattform för cirka 4 000 berörda parter för att diskutera de tekniska och samhälleliga konsekvenserna av AI, vilket kulminerade i en årlig AI-församling.

Vitboken om AI vidareutvecklade denna inkluderande strategi och ledde till kommentarer från mer än 1 250 berörda parter, inklusive ytterligare över 450 ståndpunktsdokument. Till följd av detta offentliggjorde kommissionen en inledande konsekvensbedömning, som i sin tur gav upphov till mer än 130 kommentarer[27]. **Ytterligare arbetsseminarier och evenemang för berörda parter** anordnades också och resultaten från dem stöder analysen i konsekvensbedömningen och de politiska val som görs i detta förslag[28]. En **extern studie** beställdes också för att bidra till konsekvensbedömningen.

3.3. Konsekvensbedömning

I linje med sin politik för bättre lagstiftning har kommissionen gjort en konsekvensbedömning av detta förslag som har granskats av kommissionens nämnd för lagstiftningskontroll. Den 16 december 2020 hölls ett möte med nämnden för lagstiftningskontroll, vilket följdes av ett negativt yttrande. Efter en omfattande översyn av konsekvensbedömningen till följd av kommentarerna och ett nytt inlämnande av konsekvensbedömningen avgav nämnden för lagstiftningskontroll ett positivt yttrande den 21 mars 2021. Yttrandena från nämnden för lagstiftningskontroll, rekommendationerna och en förklaring av hur de har beaktats presenteras i bilaga 1 till konsekvensbedömningen.

Kommissionen undersökte olika politiska alternativ för att uppnå förslagets allmänna mål, dvs. att **säkerställa en väl fungerande inre marknad** genom att skapa förutsättningar för utveckling och användning av tillförlitlig AI i unionen.

Följande fyra politiska alternativ med olika grader av regleringsåtgärder bedömdes:

- **Alternativ 1**: Genom ett EU-lagstiftningsinstrument inrättas ett frivilligt märkningssystem.
- **Alternativ 2:** En sektorsinriktad ad hoc-strategi.
- **Alternativ 3**: Genom ett övergripande EU-lagstiftningsinstrument införs en proportionerlig riskbaserad metod.
- **Alternativ 3+**: Genom ett övergripande EU-lagstiftningsinstrument införs en proportionerlig riskbaserad metod + uppförandekoder för AI-system som inte utgör hög risk.
- **Alternativ 4**: Genom ett övergripande EU-lagstiftningsinstrument fastställs obligatoriska krav för alla AI-system, oavsett vilken risk de utgör.

I enlighet med kommissionens vedertagna metod utvärderades varje alternativ med tanke på ekonomiska och samhälleliga konsekvenser, med särskild inriktning på konsekvenser för de

---

25 AI-expertgruppen, *Bedömningslista för tillförlitlig artificiell intelligens för självbedömning*, 2020.

26 AI-alliansen är ett flerpartsforum som lanserades i juni 2018, AI-alliansen https://ec.europa.eu/digital-single-market/en/european-ai-alliance

27 Europeiska kommissionen, *Inledande konsekvensbedömning av ett förslag till Europaparlamentets och rådets rättsakt om krav på artificiell intelligens*.

28 För närmare uppgifter om alla samråd som har genomförts, se bilaga 2 till konsekvensbedömningen.

grundläggande rättigheterna. Det föredragna alternativet är alternativ 3+, ett regelverk som endast omfattar AI-system med hög risk, med möjlighet för alla leverantörer av AI-system som inte utgör hög risk att följa en uppförandekod. Kraven kommer att gälla data, dokumentation och spårbarhet, tillhandahållande av information och transparens, mänsklig tillsyn samt robusthet och noggrannhet och skulle vara obligatoriska för AI-system med hög risk. Företag som inför uppförandekoder för andra AI-system skulle göra detta frivilligt.

Det föredragna alternativet ansågs vara lämpligt för att det på effektivast möjliga sätt kan bidra till att uppnå målen för detta förslag. Genom att kräva en begränsad men ändå effektiv uppsättning åtgärder från AI-utvecklare och AI-användare begränsar det föredragna alternativet riskerna för kränkningar av grundläggande rättigheter och människors säkerhet och främjar effektiv övervakning och efterlevnad, genom att kraven endast inriktas på system där det finns en hög risk för att sådana överträdelser kan inträffa. Detta alternativ innebär sålunda att efterlevnadskostnaderna hålls så låga som möjligt och därigenom undviks att spridningen i onödan blir långsammare på grund av högre priser och efterlevnadskostnader. För att hantera eventuella nackdelar för små och medelstora företag innehåller detta alternativ flera bestämmelser för att stödja deras uppfyllande av kraven och minska deras kostnader, inbegripet inrättandet av regulatoriska sandlådor och skyldigheten att beakta små och medelstora företags intressen när avgifterna för bedömning av överensstämmelse fastställs.

Det föredragna alternativet kommer att öka människors förtroende för AI, företagen kommer att få större rättslig säkerhet och medlemsstaterna kommer inte att ha skäl att vidta ensidiga åtgärder som skulle kunna fragmentera den inre marknaden. Den inre marknaden för AI kommer sannolikt att blomstra till följd av ökad efterfrågan tack vare ökat förtroende, fler befintliga erbjudanden tack vare rättslig säkerhet och avsaknaden av hinder för gränsöverskridande rörlighet för AI-system. Europeiska unionen kommer att fortsätta att utveckla ett snabbt växande AI-ekosystem av innovativa tjänster och produkter som integrerar AI-teknik eller fristående AI-system, vilket leder till ökad digital autonomi.

Företag eller offentliga myndigheter som utvecklar eller använder AI-tillämpningar som utgör en hög risk för medborgarnas säkerhet eller grundläggande rättigheter måste uppfylla särskilda krav och skyldigheter. Uppfyllandet av dessa krav skulle medföra kostnader på cirka 6 000–7 000 EUR fram till 2025 för tillhandahållandet av ett genomsnittligt AI-system med hög risk och som kostar ca 170 000 EUR. För AI-användare skulle det också uppkomma årliga kostnader för den tid som används för att säkerställa mänsklig tillsyn när så är lämpligt, beroende på användningsfallet. Dessa har beräknats till cirka 5 000–8 000 EUR per år. Kontrollkostnaderna kan uppgå till ytterligare 3 000–7 500 EUR för leverantörer av AI som utgör hög risk. Företag eller offentliga myndigheter som utvecklar eller använder AI-tillämpningar som inte klassificeras ha hög risk skulle endast ha minimala informationsskyldigheter. De skulle dock kunna välja att gå samman med andra och tillsammans anta en uppförandekod för att följa lämpliga krav och säkerställa att deras AI-system är tillförlitliga. I ett sådant fall skulle kostnaderna som högst vara lika höga som för AI-system med hög risk, men förmodligen lägre.

De politiska alternativens konsekvenser för olika kategorier av berörda parter (ekonomiska aktörer/företag; organ för bedömning av överensstämmelse, standardiseringsorgan och andra offentliga organ; forskare) förklaras i detalj i bilaga 3 till den konsekvensbedömning som ligger till grund för detta förslag.

3.4. Lagstiftningens ändamålsenlighet och förenkling

I detta förslag fastställs skyldigheter som kommer att gälla för leverantörer och användare av AI-system med hög risk. För leverantörer som utvecklar och släpper ut sådana system på unionsmarknaden kommer det att skapas rättslig säkerhet och säkerställas att det inte uppstår

några hinder för ett gränsöverskridande tillhandahållande av AI-relaterade tjänster och produkter. För företag som använder AI kommer förtroendet bland deras kunder att främjas. För nationella offentliga förvaltningar kommer allmänhetens förtroende för användningen av AI att främjas och efterlevnadsmekanismerna att stärkas (genom att införa en europeisk samordningsmekanism, tillhandahålla lämplig kapacitet och underlätta revisioner av AI-system med nya krav på dokumentation, spårbarhet och transparens). Dessutom kommer ramen att omfatta särskilda åtgärder till stöd för innovation, inbegripet regulatoriska sandlådor och särskilda åtgärder för att stödja småskaliga användare och leverantörer av AI-system med hög risk att följa de nya reglerna.

Förslaget syftar också specifikt till att stärka Europas konkurrenskraft och industriella bas inom AI. Full överensstämmelse säkerställs med befintlig sektorsspecifik unionslagstiftning som är tillämplig på AI-system (t.ex. för produkter och tjänster), vilket kommer att öka tydligheten och förenkla efterlevnaden av de nya reglerna.

3.5. Grundläggande rättigheter

Användningen av AI med dess specifika egenskaper (t.ex. bristande insyn, komplexitet, beroende av data, autonomt beteende) kan inverka negativt på ett antal grundläggande rättigheter som fastställs i EU-stadgan om de grundläggande rättigheterna (*stadgan*). Detta förslag syftar till att säkerställa en hög skyddsnivå för dessa grundläggande rättigheter och syftar till att hantera olika riskkällor genom en tydligt definierad riskbaserad metod. Med en uppsättning krav på tillförlitlig AI och proportionerliga skyldigheter för alla aktörer i värdekedjan kommer förslaget att stärka och främja skyddet av de rättigheter som skyddas av stadgan: rätten till människans värdighet (artikel 1), respekt för privatlivet och skydd av personuppgifter (artiklarna 7 och 8), icke-diskriminering (artikel 21) och jämställdhet mellan kvinnor och män (artikel 23). Den syftar till att förhindra en hämmande verkan på rätten till yttrandefrihet (artikel 11) och mötesfrihet (artikel 12), att säkerställa skyddet av rätten till ett effektivt rättsmedel och till en opartisk domstol, rätten till försvar och presumtion för oskuld (artiklarna 47 och 48) samt den allmänna principen om god förvaltning. Dessutom kommer förslaget, i den mån det är tillämpligt på vissa områden, att inverka positivt på rättigheterna för ett antal särskilda grupper, såsom arbetstagarnas rätt till rättvisa arbetsförhållanden (artikel 31), en hög konsumentskyddsnivå (artikel 28), barnets rättigheter (artikel 24) och integrering av personer med funktionsnedsättning (artikel 26). Rätten till en hög miljöskyddsnivå och en förbättring av miljöns kvalitet (artikel 37) är också relevant, även när det gäller människors hälsa och säkerhet. Skyldigheterna som gäller förhandstester, riskhantering och mänsklig tillsyn kommer också att underlätta respekten för andra grundläggande rättigheter genom att minimera risken för felaktiga eller snedvridna beslut med stöd av AI på kritiska områden såsom utbildning, sysselsättning, viktiga tjänster, brottsbekämpning och rättsväsendet. Om kränkningar av de grundläggande rättigheterna fortfarande förekommer kommer det att bli möjligt för berörda personer att få effektiv rättslig prövning genom att säkerställa transparens och spårbarhet i AI-systemen i kombination med kraftfulla efterhandskontroller.

Genom detta förslag införs vissa begränsningar av näringsfriheten (artikel 16) och friheten för konsten och vetenskapen (artikel 13) för att säkerställa överensstämmelse med tvingande hänsyn till allmänintresset, såsom hälsa, säkerhet, konsumentskydd och skydd av andra grundläggande rättigheter (”ansvarsfull innovation”) när AI-teknik med hög risk utvecklas och används. Dessa begränsningar är proportionerliga och begränsade till vad som är absolut nödvändigt för att förebygga och mildra allvarliga säkerhetsrisker och sannolika kränkningar av de grundläggande rättigheterna.

De ökade transparenskraven kommer inte heller att påverka rätten till skydd av immateriell egendom på ett oproportionerligt sätt (artikel 17.2), eftersom de kommer att begränsas till

endast det minimum av information som krävs för att enskilda personer ska kunna utöva sin rätt till ett effektivt rättsmedel och till nödvändig transparens gentemot tillsyns- och kontrollmyndigheterna, i enlighet med deras mandat. Allt utlämnande av information kommer att ske i enlighet med relevant lagstiftning på området, inbegripet direktiv 2016/943 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs. När offentliga myndigheter och anmälda organ behöver få tillgång till konfidentiell information eller källkod för att kontrollera efterlevnaden av väsentliga skyldigheter, omfattas de av bindande tystnadsplikt.

4. BUDGETKONSEKVENSER

Medlemsstaterna måste utse tillsynsmyndigheter som har ansvar för att genomföra de rättsliga kraven. Deras tillsynsfunktion skulle kunna baseras på befintliga strukturer, till exempel när det gäller organ för bedömning av överensstämmelse eller marknadsövervakning, men skulle kräva tillräcklig teknisk expertis och tillräckliga personalresurser och ekonomiska resurser. Beroende på den befintliga strukturen i varje medlemsstat skulle detta resursbehov kunna uppgå till 1–25 heltidsekvivalenter per medlemsstat.

En detaljerad översikt över kostnaderna finns i den finansieringsöversikt som åtföljer detta förslag.

5. ÖVRIGA INSLAG

5.1. Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering

För att säkerställa att förslaget på ett effektivt sätt uppnår sina specifika mål är det avgörande att en robust övervaknings- och utvärderingsmekanism kan tillhandahållas. Kommissionen kommer att ansvara för övervakningen av förslagets effekter. Kommissionen kommer att inrätta ett system för registrering av fristående AI-tillämpningar med hög risk i en offentlig EU-omfattande databas. Denna registrering kommer också att göra det möjligt för behöriga myndigheter, användare och andra intresserade att kontrollera om AI-systemet med hög risk uppfyller kraven i förslaget och utöva förstärkt tillsyn över de AI-system som utgör hög risk för de grundläggande rättigheterna. För att få in uppgifter i denna databas kommer AI-leverantörer att vara skyldiga att tillhandahålla meningsfull information om sina system och om den bedömning av överensstämmelse som utförs för dessa system.

AI-leverantörer kommer dessutom att vara skyldiga att informera de nationella behöriga myndigheterna om allvarliga incidenter eller funktionsstörningar som utgör brott mot skyldigheterna som rör de grundläggande rättigheterna så snart de får kännedom om dem, samt om återkallelser eller tillbakadraganden av AI-system från marknaden. De nationella behöriga myndigheterna kommer sedan att utreda incidenterna eller funktionsstörningarna, samla in all nödvändig information och regelbundet översända den till kommissionen med lämpliga metadata. Kommissionen kommer att komplettera denna information om incidenter med en omfattande analys av den övergripande marknaden för AI.

Kommissionen kommer att offentliggöra en rapport som utvärderar och ser över den föreslagna ramen för AI fem år efter den dag då den börjar tillämpas.

5.2. Ingående redogörelse för de specifika bestämmelserna i förslaget

5.2.1. TILLÄMPNINGSOMRÅDE OCH DEFINITIONER (AVDELNING I)

I **avdelning I** fastställs förordningens innehåll och tillämpningsområdet för de nya regler som omfattar utsläppande på marknaden, ibruktagande och användning av AI-system. Den

innehåller också de definitioner som används i hela instrumentet. Definitionen av AI-system i den rättsliga ramen syftar till att vara så teknikneutral och framtidssäkrad som möjligt, med beaktande av den snabba tekniska utvecklingen och marknadsutvecklingen för AI. För att skapa den rättssäkerhet som krävs kompletteras avdelning I av bilaga I, som innehåller en detaljerad förteckning över metoder och tekniker för utveckling av AI som kommissionen kommer att anpassa till ny teknisk utveckling. Nyckelaktörer i hela AI-värdekedjan, såsom leverantörer och användare av AI-system, vilket omfattar både offentliga och privata aktörer för att säkerställa lika villkor, är också tydligt definierade.

5.2.2. FÖRBJUDNA TILLÄMPNINGAR AV ARTIFICIELL INTELLIGENS (AVDELNING II)

I **avdelning II** ingår en förteckning över förbjuden AI. Förordningen följer en riskbaserad metod där man skiljer mellan användning av AI som skapar i) oacceptabel risk, ii) hög risk och iii) låg eller minimal risk. Förteckningen över förbjudna metoder i avdelning II omfattar alla AI-system vars användning anses strida mot unionens värden, till exempel genom att kränka de grundläggande rättigheterna. Förbuden omfattar metoder som har en betydande potential att manipulera personer genom subliminal teknik som människor inte är medvetna om eller som utnyttjar sårbarheter hos specifika utsatta grupper, såsom barn eller personer med funktionsnedsättning, i syfte att väsentligt snedvrida deras beteende på ett sätt som sannolikt kommer att orsaka dem eller en annan person psykisk eller fysisk skada. Andra manipulativa eller utnyttjande metoder som påverkar vuxna och som kan underlättas av AI-system skulle kunna omfattas av befintlig lagstiftning om dataskydd, konsumentskydd och digitala tjänster som garanterar att fysiska personer är ordentligt informerade och har fritt val att inte blir föremål för profilering eller andra metoder som kan påverka deras beteende. Enligt förslaget är AI-baserad social poängsättning för allmänna ändamål som utförs av offentliga myndigheter också förbjuden. Slutligen är det också förbjudet att använda biometriska fjärridentifieringssystem i realtid på allmänt tillgängliga platser för brottsbekämpningsändamål, utom i vissa begränsade undantagsfall.

5.2.3. AI-SYSTEM MED HÖG RISK (AVDELNING III)

I **avdelning III** ingår särskilda regler för AI-system som medför en hög risk för fysiska personers hälsa och säkerhet eller grundläggande rättigheter. I linje med en riskbaserad metod är dessa AI-system med hög risk tillåtna på den europeiska marknaden under förutsättning att vissa obligatoriska krav uppfylls och en förhandsbedömning av överensstämmelse görs. Klassificeringen av att ett AI-system utgör hög risk baseras på det avsedda ändamålet med AI-systemet, i linje med befintlig produktsäkerhetslagstiftning. Klassificeringen som system med hög risk beror därför inte bara på den funktion som AI-systemet fyller, utan också på specifika syftena med och formerna för användningen av systemet.

I avdelning III kapitel 1 fastställs klassificeringsreglerna och följande två huvudkategorier av AI-system med hög risk:

- AI-system som är avsedda att användas som säkerhetskomponenter i produkter som är föremål för förhandsbedömning av överensstämmelse från tredje part.
- Andra fristående AI-system med konsekvenser för framför allt de grundläggande rättigheterna och som uttryckligen förtecknas i bilaga III.

Förteckningen över AI-system med hög risk i bilaga III innehåller ett begränsat antal AI-system vars risker redan har förverkligats eller sannolikt kommer att förverkligas inom en nära framtid. För att säkerställa att förordningen kan anpassas till nya användningar och tillämpningar av AI kan kommissionen, genom att tillämpa en uppsättning kriterier och

riskbedömningsmetoder, utöka förteckningen över AI-system med hög risk som används inom vissa på förhand fastställda områden.

I kapitel 2 fastställs de rättsliga kraven för AI-system med hög risk när det gäller data och dataförvaltning, dokumentation och arkivering, transparens och tillhandahållande av information till användare, mänsklig tillsyn, robusthet, noggrannhet och säkerhet. De föreslagna minimikraven representerar redan den nyaste utvecklingen för många ansvarskännande aktörer och är resultatet av två års förberedande arbete, som bygger på AI-expertgruppens etiska riktlinjer[29] och använts i en pilotfas av fler än 350 organisationer[30]. De är också i hög grad förenliga med andra internationella rekommendationer och principer, vilket säkerställer att den föreslagna ramen för AI är förenlig med de ramar som antagits av EU:s internationella handelspartner. De exakta tekniska lösningarna för att uppnå överensstämmelse med dessa krav kan tillhandahållas genom standarder eller andra tekniska specifikationer eller på annat sätt utvecklas i enlighet med allmän ingenjörsvetenskap eller vetenskaplig kunskap efter gottfinnande av leverantören av AI-systemet. Denna flexibilitet är särskilt viktig eftersom den gör det möjligt för leverantörer av AI-system att välja hur de ska uppfylla sina krav, med beaktande av den senaste tekniska och vetenskapliga utvecklingen på området.

I kapitel 3 ingår en tydlig uppsättning övergripande skyldigheter för leverantörer av AI-system med hög risk. Proportionerliga skyldigheter åläggs också användare och andra deltagare i hela AI-värdekedjan (t.ex. importörer, distributörer, ombud).

I kapitel 4 fastställs ramen för hur anmälda organ deltar som oberoende tredje parter i förfaranden för bedömning av överensstämmelse, medan kapitel 5 innehåller en detaljerad redogörelse för de förfaranden för bedömning av överensstämmelse som ska följas för varje typ av AI-system med hög risk. Metoden för bedömning av överensstämmelse syftar till att minimera bördan för både ekonomiska aktörer och anmälda organ, vars kapacitet måste ökas gradvis med tiden. AI-system som är avsedda att användas som säkerhetskomponenter i produkter som regleras i den nya lagstiftningsramen (t.ex. maskiner, leksaker, medicintekniska produkter osv.) kommer att omfattas av samma mekanismer för efterlevnad och kontroll i efterhand som de produkter som de ingår i. Den viktigaste skillnaden är att förhands- och efterhandsmekanismerna kommer att säkerställa överensstämmelse inte bara med de krav som fastställs i sektorslagstiftningen, utan också med de krav som fastställs i denna förordning.

När det gäller de fristående AI-system med hög risk som avses i bilaga III kommer ett nytt system för efterlevnad och verkställighet att inrättas. Detta följer modellen i den nya lagstiftningsramen, där lagstiftningen genomförs genom interna kontroller utförda av leverantörerna, med undantag för system för biometrisk fjärridentifiering som skulle bli föremål för tredjepartsbedömning av överensstämmelse. En omfattande förhandsbedömning av överensstämmelse genom interna kontroller, i kombination med en kraftfull efterhandskontroll, skulle kunna vara en effektiv och rimlig lösning för dessa system, med tanke på regleringsåtgärdernas tidiga fas och det faktum att AI-sektorn är mycket innovativ och att expertis för revision byggs upp först nu. En bedömning genom interna kontroller av fristående AI-system med hög risk skulle kräva en fullständig, effektiv och korrekt dokumenterad förhandsefterlevnad av alla krav i förordningen och efterlevnad av robusta kvalitets- och riskhanteringssystem samt övervakning av produkter som släppts ut på

[29] Högnivåexpertgruppen för artificiell intelligens, *Etiska riktlinjer för tillförlitlig AI*, 2019.

[30] De godkändes också av kommissionen i dess meddelande från 2019 om en människocentrerad strategi för AI.

marknaden. När leverantören har utfört den relevanta bedömningen av överensstämmelse bör den registrera dessa fristående AI-system med hög risk i en EU-databas som kommer att förvaltas av kommissionen för att öka den offentliga transparensen och tillsynen och stärka de behöriga myndigheternas efterhandstillsyn. För att uppnå överensstämmelse med den befintliga produktsäkerhetslagstiftningen kommer bedömningar av överensstämmelse av AI-system som är säkerhetskomponenter i produkter däremot att följa ett system med förfaranden för tredjepartsbedömning av överensstämmelse, som redan inrättats enligt relevant sektorsspecifik produktsäkerhetslagstiftning. Förnyade förhandsbedömningar av överensstämmelsen kommer att behövas vid betydande ändringar av AI-systemen (och i synnerhet ändringar som går utöver vad leverantören på förhand fastställt i sin tekniska dokumentation och som kontrolleras i samband med förhandsbedömningen av överensstämmelse).

5.2.4. TRANSPARENSKRAV FÖR VISSA AI-SYSTEM (AVDELNING IV)

Genom **avdelning IV** tas det hänsyn till de särskilda risker för manipulation som vissa AI-system medför. Transparenskrav kommer att gälla för system som i) interagerar med människor, ii) används för att läsa av känslor eller fastställa en koppling till (sociala) kategorier baserade på biometriska uppgifter eller iii) genererar eller manipulerar innehåll (”deepfake”). När personer interagerar med ett AI-system, eller deras känslor eller egenskaper uttyds automatiskt, måste de informeras om detta. Om ett AI-system används för att generera eller manipulera bild-, ljud- eller videoinnehåll som på ett märkbart sätt liknar autentiskt innehåll bör det finnas en skyldighet att avslöja att innehållet har skapats på automatiserad väg, med förbehåll för undantag för legitima ändamål (brottsbekämpning, yttrandefrihet). Detta gör det möjligt för personer att göra välgrundade val eller backa från situationen.

5.2.5. ÅTGÄRDER TILL STÖD FÖR INNOVATION (AVDELNING V)

Avdelning V bidrar till målet att skapa en rättslig ram som är innovationsvänlig, framtidssäker och resilient mot störningar. Därför uppmuntras de nationella behöriga myndigheterna att inrätta regulatoriska sandlådor och fastställa en grundläggande ram för styrning, tillsyn och ansvar. Genom regulatoriska sandlådor för AI skapas en kontrollerad miljö för att testa innovativ teknik under en begränsad tid på grundval av en testplan som överenskommits med de behöriga myndigheterna. I avdelning V ingår också åtgärder för att minska regelbördan för små och medelstora företag samt nystartade företag.

5.2.6. STYRNING OCH GENOMFÖRANDE (AVDELNINGARNA VI, VII OCH VII)

Genom **avdelning VI** inrättas styrningssystemen på unionsnivå och nationell nivå. På unionsnivå inrättas genom förslaget en europeisk nämnd för artificiell intelligens (*nämnden*) som består av företrädare för medlemsstaterna och kommissionen. Nämnden kommer att underlätta ett smidigt, effektivt och harmoniserat genomförande av denna förordning genom att bidra till ett effektivt samarbete mellan de nationella tillsynsmyndigheterna och kommissionen samt tillhandahålla råd och sakkunskap till kommissionen. Den kommer också att samla in och utbyta bästa praxis mellan medlemsstaterna.

På nationell nivå måste medlemsstaterna utse en eller flera nationella behöriga myndigheter, bland annat den nationella tillsynsmyndigheten, för att övervaka tillämpningen och genomförandet av förordningen. Europeiska datatillsynsmannen kommer att verka som behörig myndighet för tillsyn av unionens institutioner, byråer och organ som omfattas av denna förordning.

Avsikten med **avdelning VII** är att underlätta kommissionens och de nationella myndigheternas övervakningsarbete genom att inrätta en EU-omfattande databas för fristående AI-system med hög risk som huvudsakligen har konsekvenser för de

grundläggande rättigheterna. Databasen kommer att upprätthållas av kommissionen och förses med data från leverantörerna av AI-systemen, som kommer att vara skyldiga att registrera sina system innan de släpps ut på marknaden eller på annat sätt tas i bruk.

I **avdelning VIII** fastställs övervaknings- och rapporteringsskyldigheter för leverantörer av AI-system när det gäller övervakning efter utsläppandet på marknaden samt rapportering och utredning av AI-relaterade incidenter och funktionsstörningar. Marknadskontrollmyndigheterna skulle också kontrollera marknaden och undersöka efterlevnaden av skyldigheterna och kraven för alla AI-system med hög risk som redan släppts ut på marknaden. Marknadskontrollmyndigheterna skulle ha alla befogenheter enligt förordning (EU) 2019/1020 om marknadskontroll. Efterhandskontroller bör säkerställa att offentliga myndigheter, när AI-systemet väl har släppts ut på marknaden, har befogenheter och resurser att ingripa om AI-system skapar oväntade risker som kräver snabba åtgärder. De kommer också att övervaka att operatörerna uppfyller sina relevanta skyldigheter enligt förordningen. I förslaget föreskrivs inte ett automatiskt inrättande av ytterligare organ eller myndigheter på medlemsstatsnivå. Medlemsstaterna kan därför utse (och utnyttja sakkunskapen hos) befintliga sektorsmyndigheter, som skulle få befogenhet att övervaka och verkställa bestämmelserna också i denna förordning.

Allt detta påverkar inte tillämpningen av det befintliga systemet och fördelningen av befogenheter för efterhandskontroll av skyldigheter som gäller de grundläggande rättigheterna i medlemsstaterna. När det är nödvändigt för deras uppdrag kommer de befintliga tillsyns- och kontrollmyndigheterna också att ha befogenhet att begära och få tillgång till all dokumentation som bevaras i enlighet med denna förordning och vid behov begära att marknadskontrollmyndigheterna organiserar testning av AI-system med hög risk med tekniska medel.

5.2.7. UPPFÖRANDEKODER (AVDELNING IX)

Genom **avdelning IX** inrättas en ram för utarbetande av uppförandekoder som syftar till att uppmuntra leverantörer av AI-system som inte utgör hög risk att frivilligt tillämpa de obligatoriska kraven för AI-system med hög risk (i enlighet med avdelning III). Leverantörer av AI-system som inte utgör hög risk kan själva skapa och genomföra uppförandekoder. I dessa koder kan det också ingå frivilliga åtaganden avseende exempelvis miljöhållbarhet, tillgänglighet för personer med funktionsnedsättning, berörda parters deltagande i utformningen och utvecklingen av AI-system samt mångfald i utvecklingsteamen.

5.2.8. SLUTBESTÄMMELSER (AVDELNINGARNA X, XI OCH XII)

I **avdelning X** betonas alla parters skyldighet att respektera konfidentialiteten för information och uppgifter och fastställs regler för utbyte av information som erhållits under genomförandet av förordningen. I avdelning X ingår också åtgärder för att säkerställa ett effektivt genomförande av förordningen genom effektiva, proportionella och avskräckande sanktioner för överträdelser av bestämmelserna.

I **avdelning XI** fastställs regler för utövande av delegerade befogenheter och genomförandebefogenheter. Förslaget ger kommissionen befogenhet att vid behov anta genomförandeakter för att säkerställa en enhetlig tillämpning av förordningen eller delegerade akter för att uppdatera eller komplettera förteckningarna i bilagorna I–VII.

I **avdelning XII** ingår en skyldighet för kommissionen att regelbundet bedöma behovet av en uppdatering av bilaga III och att regelbundet utarbeta rapporter om utvärderingen och översynen av förordningen. Den innehåller också slutbestämmelser, inklusive en differentierad övergångsperiod som gäller det första tillämpningsdatumet för förordningen för att underlätta ett smidigt genomförande för alla berörda parter.

2021/0106 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

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

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 16 och 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[31],

med beaktande av Regionkommitténs yttrande[32],

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) Syftet med denna förordning är att förbättra den inre marknadens funktionssätt genom att fastställa en enhetlig rättslig ram för i synnerhet utveckling, 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 aktörer som utvecklar 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

[31] EUT C […], […], s. […].
[32] EUT C […], […], s. […].

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 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 stöder denna förordning unionens mål att bli världsledande inom utvecklingen av säker, tillförlitlig och etisk artificiell intelligens, såsom fastställts av Europeiska rådet[33], och säkerställer skyddet av etiska principer, vilket särskilt har begärts av Europaparlamentet[34].

(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 programvarans viktigaste funktionella egenskaper, i synnerhet förmågan att, för en viss uppsättning mänskligt definierade syften, generera sådana utdata som innehåll, prognoser eller rekommendationer, eller beslut som påverkar den miljö som systemet interagerar med, i en fysisk eller digital dimension. 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). Definitionen av AI-system bör kompletteras med

---

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

34 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)).

en förteckning över specifika tekniker och metoder som används för utvecklingen av AI-system, vilken bör uppdateras i takt med marknadsutvecklingen och den tekniska utvecklingen genom att kommissionen antar delegerade akter om ändring av denna förteckning.

(7) Begreppet biometriska uppgifter, som används i denna förordning är i linje med och bör tolkas i överensstämmelse med begreppet biometriska uppgifter enligt definitionen i artikel 4.14 i Europaparlamentets och rådets förordning (EU) 2016/679[35], artikel 3.18 i Europaparlamentets och rådets förordning (EU) 2018/1725[36] och artikel 3.13 i Europaparlamentets och rådets direktiv (EU) 2016/680[37].

(8) Begreppet system för biometrisk fjärridentifiering enligt denna förordning bör definieras utifrån funktion, som ett AI-system avsett för fjärridentifiering av fysiska personer genom jämförelse mellan en persons biometriska uppgifter och biometriska uppgifter i en referensdatabas, och utan någon förhandskunskap om huruvida den berörda personen kommer att vara närvarande och kan identifieras, oavsett den specifika teknik, process eller typ av biometriska uppgifter som används. Mot bakgrund av systemens olika kännetecken och de olika sätt som de används på, liksom de olika risker som är involverade, bör en åtskillnad göras mellan system för biometrisk identifiering ”i realtid” och ”i efterhand”. 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 allmänheten, oavsett om platsen i fråga är i privat eller offentlig ägo. Därmed omfattar begreppet inte platser som är av privat art och som normalt inte är fritt tillgängliga för tredje part, inbegripet brottsbekämpande myndigheter, om inte dessa parter särskilt har bjudits in eller getts tillåtelse, såsom bostäder, privata klubbar, kontor, lager och fabriker. Onlineplatser omfattas inte heller eftersom de inte är fysiska platser. Enbart det faktum att vissa villkor kan gälla för att

---

35 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).

36 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).

37 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).

få tillträde till en viss plats, såsom inträdesbiljetter eller åldersgränser, betyder inte att platsen inte anses allmänt tillgänglig enligt denna förordning. Vid sidan av sådana offentliga platser som gator, berörda delar av offentliga byggnader och de flesta transportinfrastrukturer är normalt också sådana platser som biografer, teatrar, affärer och köpcentrum tillgängliga för allmänheten. 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 aktör 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 och vars effekter påverkar fysiska personer som befinner sig i unionen. 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 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.

(12) Denna förordning bör också tillämpas på unionens institutioner, kontor, organ och byråer när de agerar som tillhandahållare eller användare av AI-system. AI-system som uteslutande utvecklas eller används för militära ändamål bör undantas från denna förordnings tillämpningsområde i de fall då användningen faller under den gemensamma utrikes- och säkerhetspolitikens exklusiva behörighet vilken regleras genom avdelning V i fördraget om Europeiska unionen (EU-fördraget). 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].

(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) Utsläppandet på marknaden och ibruktagandet eller användningen av vissa AI-system avsedda att snedvrida mänskligt beteende, och som sannolikt kan medföra fysisk eller psykisk skada, bör förbjudas. Sådana AI-system använder subliminala komponenter som inte kan uppfattas av individer eller utnyttjar sårbarheter hos barn och människor på grund av deras ålder eller fysiska eller mentala funktionsnedsättningar. De gör detta i avsikt att väsentligt snedvrida en persons beteende på ett sätt som skadar eller sannolikt kan skada den personen eller en annan person. Avsikten kan inte presumeras om snedvridningen av mänskligt beteende är resultatet av faktorer utanför AI-systemet vilka är utom leverantörens eller användarens kontroll. Forskning för legitima syften som är relaterade till sådana AI-system bör inte hindras av förbudet, om denna forskning inte innefattar användning av AI-system i människa-maskin-relationer som utsätter fysiska personer för skada och om den utförs i enlighet med erkända etiska normer för vetenskaplig forskning.

(17) AI-system som tillhandahåller social poängsättning av fysiska personer för allmänna syften för offentliga myndigheter, eller på deras vägnar, 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 personers tillförlitlighet 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. Sådana AI-system bör därför förbjudas.

(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 tre 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, och avslöjande, lokalisering, identifiering eller lagföring av gärningsmän till eller misstänkta för brott som avses i rådets rambeslut 2002/584/RIF[38], 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.

(20) För att säkerställa att dessa system används på ett ansvarfullt och proportionerligt sätt är det också viktigt att fastställa att hänsyn bör tas till vissa faktorer i var och en av de tre 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 tre 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 före användningen, utom 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

[38] 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).

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 på allmänt tillgänglig plats i brottsbekämpningssyfte som regleras av denna förordning, inbegripet när sådana system används av behöriga myndigheter på allmänt tillgänglig plats för andra syften än brottsbekämpning, bör även fortsättningsvis uppfylla alla krav som följer av artikel 9.1 i förordning (EU) 2016/679, artikel 10.1 i förordning (EU) 2018/1725 och artikel 10 i direktiv (EU) 2016/680, såsom tillämpligt.

(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.2 och d.3 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.2 och d.3 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[39], Europaparlamentets och rådets förordning (EU) nr 167/2013[40], Europaparlamentets och rådets förordning

[39] 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).

[40] 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).

(EU) nr 168/2013[41], Europaparlamentets och rådets direktiv 2014/90/EU[42], Europaparlamentets och rådets direktiv (EU) 2016/797[43], Europaparlamentets och rådets förordning (EU) 2018/858[44], Europaparlamentets och rådets förordning (EU) 2018/1139[45] och Europaparlamentets och rådets förordning (EU) 2019/2144[46], 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.

(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

---

41 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).

42 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).

43 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).

44 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).

45 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).

46 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).

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[47] och Europaparlamentets och rådets förordning (EU) 2017/746[48], i vilka tredjepartsbedömning av överensstämmelse föreskrivs för produkter med medelhög risk och hög risk.

(32) När det gäller fristående AI-system, med vilket avses andra AI-system med hög risk än sådana som utgör säkerhetskomponenter i produkter, eller AI-system 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.

(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, 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 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.

(35) AI-system som används för yrkesutbildning eller annan utbildning, i synnerhet när det gäller fastställandet av personers tillgång till institutioner för yrkesutbildning eller annan utbildning, eller för att utvärdera personer tester som ett led i eller som en förutsättning för deras utbildning, 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, övervakning eller utvärdering av personer i arbetsrelaterade avtalsförhållanden, bör också klassificeras som hög risk, eftersom dessa system märkbart kan påverka framtida karriärutsikter och

[47] 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).

[48] 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).

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 som utnyttjas av småskaliga leverantörer för egen användning bör undantas, mot bakgrund av effekternas mycket begränsade omfattning och de tillgängliga alternativen på marknaden. Fysiska personer som ansöker om eller erhåller 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 kan de 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.

(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, upptäcka ”deepfake”, 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 och i samband med brottsanalys som avser fysiska personer. AI-system som är specifikt avsedda att användas för administrativa förfaranden hos skattemyndigheter och tullmyndigheter 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, för att kontrollera äktheten i fysiska personers relevanta handlingar, 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[49], Europaparlamentets och rådets förordning (EG) nr 810/2009[50] och annan relevant lagstiftning.

(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

[49] 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).

[50] 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).

klassificera sådana AI-system som är avsedda att hjälpa de rättsliga myndigheterna att undersöka och 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 eller fördelning av resurser.

(41) Det faktum att ett AI-system klassificerats som hög risk enligt denna förordning bör inte tolkas som att användningen av det systemet nödvändigtvis är lagligt 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.

(42) För att begränsa riskerna för användare och berörda personer från 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.

(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. Dataset för träning, validering och testning bör vara tillräckligt relevanta, representativa och felfria och kompletta i förhållande till systemets avsedda ändamål. De bör också ha lämpliga statistiska egenskaper, inbegripet vad gäller de personer eller grupper av personer på vilka AI-systemet med hög risk är avsett att användas. Dataset för träning, validering och testning bör i synnerhet, i den mån som krävs med tanke på systemens 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 betydande allmänintresse, för att säkerställa övervakning, upptäckt och korrigering av snedvridning när det gäller AI-system med hög risk.

(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.

(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, när så är lämpligt.

(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.

(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. Systemen bör vara resilienta mot risker kopplade till systemets begränsningar (dvs. felaktigheter, funktionsfel, inkonsekvenser, oväntade situationer samt sabotage som kan äventyra AI-systemets säkerhet och resultera i skadligt eller på annat sätt oönskat beteende. 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[51] om krav för ackreditering och marknadskontroll i samband med saluföring av produkter, Europaparlamentets och rådets beslut nr 768/2008/EG[52] om en gemensam ram för saluföring av produkter samt Europaparlamentets och rådets förordning (EU) 2019/1020[53] om marknadskontroll och överensstämmelse för produkter (*den nya lagstiftningsramen*).

(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.

(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.

(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 tillverkaren av slutprodukten, 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.

---

51 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).

52 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).

53 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).

(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.

(57) I linje med den nya lagstiftningsramens principer bör särskilda skyldigheter fastställas för berörda ekonomiska aktörer, såsom importörer och distributörer, för att säkerställa rättssäkerheten och främja dessa berörda aktörers regelefterlevnad.

(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.

(59) Det är lämpligt att utgå från att användaren av AI-systemet bör vara den fysiska eller juridiska person, offentliga myndighet eller den byrå eller andra organ under vars överinseende AI-systemet används, utom när AI-systemet används inom ramen för en personlig icke-yrkesmässig verksamhet.

(60) Mot bakgrund av den komplexa värdekedjan för artificiell intelligens, bör berörda tredje parter, i synnerhet sådana som är involverade i försäljning och tillhandahållande av programvara, programvaruverktyg och komponenter, förhandstränade modeller och data, eller leverantörer av nättjänster, samarbeta såsom lämpligt med leverantörer och användare för att främja deras uppfyllande av skyldigheterna enligt denna förordning och med behöriga myndigheter som inrättas i enlighet med denna förordning.

(61) Standardisering bör ha en nyckelroll för att förse leverantörerna med tekniska lösningar för att säkerställa efterlevnaden av denna förordning. Överenstämmelse med harmoniserade standarder enligt Europaparlamentets och rådets förordning (EU) nr 1025/2012[54] bör vara ett sätt för leverantörerna att visa att de uppfyller kraven i denna förordning. Kommissionen skulle dock kunna anta gemensamma tekniska specifikationer på områden där harmoniserade standarder saknas eller är otillräckliga.

(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

[54] 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).

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.

(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 utses 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.

(66) I linje med det vedertagna begreppet väsentlig ändring som avser produkter som regleras genom unionens lagstiftning om harmonisering, är det lämpligt att ett AI-system genomgår en ny bedömning av överensstämmelse vid varje ändring som kan påverka systemets överensstämmelse med denna förordning eller när systemets avsedda ändamål ändras. När det gäller AI-system som fortsätter sin ”inlärning” efter att de släppts ut på marknaden eller tagits i bruk (dvs. automatiskt anpassar sitt sätt att utföra funktioner) är det nödvändigt att föreskriva regler som fastställer att ändringar av algoritmen och dess prestanda som har förutbestämts av leverantören och som bedömts i samband med bedömningen av överensstämmelse inte ska utgöra väsentliga ändringar.

(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 sina AI-system med hög risk i en EU-databas, som upprättas och förvaltas av kommissionen. Kommissionen bör vara personuppgiftsansvarig för denna databas i enlighet med Europaparlamentets och rådets förordning (EU) 2018/1725[55]. 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.

(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, utom om detta är uppenbart utifrån omständigheterna eller användningssituationen. Fysiska personer bör också meddelas när de exponeras för ett system för känsloigenkänning eller ett system för biometrisk kategorisering. 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.

(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 dessa ”regulatoriska sandlådor” 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 och uppstartsföretag. 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

[55] 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).

sandlådor. Denna förordning bör erbjuda den rättsliga grunden för användning av personuppgifter för andra ändamål än utvecklingen av vissa AI-system i allmänhetens intresse inom regulatoriska sandlådor för AI, i linje med artikel 6.4 i förordning (EU) 2016/679 och artikel 6 i förordning (EU) 2018/1725, och utan att det påverkar tillämpningen av artikel 4.2 i direktiv (EU) 2016/680. 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.

(73) För att främja och skydda innovation är det viktigt att särskild hänsyn tas till småskaliga leverantörer och användare av AI-system. I detta syfte bör medlemsstaterna ta fram initiativ som riktar sig till dessa aktörer, bland annat vad gäller medvetandehöjande och information. De småskaliga leverantörernas särskilda intressen 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.

(74) För att minimera risker för genomförandet som följer av bristande kunskap och expertis på marknaden, och för att främja leverantörernas 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 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.

(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 ansvara för ett antal rådgivande uppgifter, däribland att utfärda yttranden, rekommendationer, råd eller vägledning om frågor som rör genomförandet av denna förordning, inbegripet när det gäller tekniska specifikationer eller befintliga standarder avseende kraven i denna förordning och råd och bistånd till kommissionen om specifika frågor som rör artificiell intelligens.

(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. För att öka den organisatoriska effektiviteten från medlemsstaternas sida och inrätta en officiell kontaktpunkt för kontakterna med allmänheten och andra motparter på medlemsstatsnivå och unionsnivå bör en nationell myndighet utses till nationell tillsynsmyndighet i varje medlemsstat.

(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 eller överträdelser av nationell lagstiftning och unionslagstiftning som skyddar grundläggande rättigheter 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. När det är nödvändigt för deras uppdrag bör nationella offentliga myndigheter eller organ, som övervakar tillämpningen av unionslagstiftning som skyddar grundläggande rättigheter, inbegripet likabehandlingsorgan, också ha tillgång till all dokumentation som skapas i enlighet med denna förordning.

(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, inbegripet i förekommande fall Europeiska centralbanken, 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. 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[56] är det också lämpligt att i de befintliga skyldigheterna och förfarandena enligt direktiv 2013/36/EU integrera förfarandet för bedömning av överensstämmelse och 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

[56] 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).

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 regleras genom direktiv 2013/36/EU.

(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 vars tillämpning är obligatorisk för AI-system med hög risk. Leverantörerna bör också uppmuntras att på frivillig grund tillämpa ytterligare krav avseende exempelvis miljöhållbarhet, 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[57] 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.

(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. 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 de tekniker och metoder som anges i bilaga I för definition av AI-system, unionens lagstiftning om harmonisering 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 kvalitetsledningssystemet 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 om bättre lagstiftning av den 13 april 2016[58]. För att säkerställa lika stor delaktighet i

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

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

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.

(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[59].

(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.

(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,

[59] Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

(c) harmoniserade transparensregler för AI-system som är avsedda att interagera med fysiska personer, system för känsloigenkänning och system för biometrisk kategorisering samt AI-system som används för att generera eller manipulera bild-, ljud- eller videoinnehåll,

(d) regler om marknadskontroll och marknadsövervakning.

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 etablerade i unionen eller i ett tredjeland,

(b) användare av AI-system när dessa användare befinner sig i unionen,

(c) leverantörer och användare av AI-system när dessa leverantörer och användare befinner sig i ett tredjeland, där de utdata som produceras av systemet används i unionen.

2. För AI-system med hög risk som utgör säkerhetskomponenter i produkter eller system, eller som själva är produkter eller system, som omfattas av tillämpningsområdet för följande akter, ska endast artikel 84 i denna förordning tillämpas:

(a) Förordning (EG) nr 300/2008.

(b) Förordning (EU) nr 167/2013.

(c) Förordning (EU) nr 168/2013.

(d) Direktiv 2014/90/EU.

(e) Direktiv (EU) 2016/797.

(f) Förordning (EU) 2018/858.

(g) Förordning (EU) 2018/1139.

(h) Förordning (EU) 2019/2144.

3. Denna förordning ska inte tillämpas på AI-system som utvecklats eller används uteslutande för militära ändamål.

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[60] [*som ska ersättas av motsvarande bestämmelser i rättsakten om digitala tjänster*].

Artikel 3
Definitioner

I denna förordning gäller följande definitioner:

(1) *system med artificiell intelligens (AI-system)*: programvara som utvecklats med en eller flera av de tekniker och metoder som förtecknas i bilaga I och som, för en viss uppsättning människodefinierade mål, kan generera utdata såsom innehåll, förutsägelser, rekommendationer eller beslut som påverkar de miljöer som de samverkar med.

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

(3) *småskalig leverantör*: en leverantör som är ett mikroföretag eller småföretag i den mening som avses i kommissionens rekommendation 2003/361/EG[61].

(4) *användare*: varje fysisk eller juridisk person, offentlig myndighet, byrå eller annat organ som under eget överinseende använder ett AI-system, utom när AI-systemet används inom ramen för en personlig icke-yrkesmässig verksamhet.

(5) *ombud*: en fysisk eller juridisk person som är etablerad i unionen och som har fått 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.

(6) *importör*: en fysisk eller juridisk person som är etablerad i unionen och som släpper ut på marknaden eller tar i bruk ett AI-system, 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 utan att påverka dess egenskaper.

(8) *operatör*: leverantören, användaren, den auktoriserade representanten, importören och 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.

---

60 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).

61 Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

(11) *ibruktagande*: leverans av ett AI-system för första användning direkt till användaren eller för eget bruk på unionsmarknaden 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, inklusive den specifika geografiska, beteendemässiga eller funktionella miljö inom vilken AI-systemet med hög risk är avsett att användas.

(16) *återkallelse av ett AI-system*: varje åtgärd som syftar till att få till stånd ett återlämnande av ett AI-system som tillhandahållits för användare till leverantören.

(17) *tillbakadragande av ett AI-system*: varje åtgärd som syftar till att förhindra distribution, exponering och utbjudande av ett AI-system.

(18) *ett AI-systems prestanda*: ett AI-systems förmåga att uppnå sitt avsedda ändamål.

(19) *anmälande myndighet*: den nationella myndighet som ansvarar för inrättandet och genomförandet av de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och för övervakning av dessa.

(20) *bedömning av överensstämmelse*: processen där det kontrolleras om kraven i avdelning III kapitel 2 i denna förordning avseende ett AI-system har uppfyllts.

(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 leder till en ändring av det avsedda ändamål för vilket AI-systemet har bedömts.

(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 i denna förordning och annan tillämplig unionslagstiftning som harmoniserar villkoren för saluföring av produkter (*unionens harmoniseringslagstiftning*) och som föreskriver sådan märkning.

(25) *övervakning efter utsläppande på marknaden*: all verksamhet som bedrivs av leverantörer av AI-system för att proaktivt 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) *gemensamma specifikationer*: ett dokument som inte är en standard och som innehåller tekniska lösningar som ger möjlighet att uppfylla vissa krav och skyldigheter som fastställs i denna förordning.

(29) *träningsdata*: data som används för att träna ett AI-system genom anpassning av dess inlärningsbara parametrar, inklusive vikterna i ett neuralt nätverk.

(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 och som möjliggör eller bekräftar den unika identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter.

(34) *system för känsloigenkänning*: ett AI-system vars syfte är att identifiera eller uttyda fysiska personers 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 såsom kön, ålder, hårfärg, ögonfärg, tatueringar, etniskt ursprung eller sexuell eller politisk läggning, på grundval av deras biometriska uppgifter.

(36) *system för biometrisk fjärridentifiering*: ett AI-system vars syfte är att identifiera fysiska personer på distans genom jämförelse av en persons biometriska uppgifter med de biometriska uppgifterna i en referensdatabas, och utan att användaren av AI-systemet i förväg känner till huruvida personen kommer att vara närvarande och kan identifieras.

(37) *system för biometrisk fjärridentifiering i realtid*: ett system för biometrisk fjärridentifiering där insamling av biometriska uppgifter, jämförelse och identifiering sker utan betydande dröjsmål. Detta omfattar inte bara omedelbar identifiering, utan även begränsade korta fördröjningar för att undvika kringgående.

(38) *system för biometrisk fjärridentifiering i efterhand*: ett annat system för biometrisk fjärridentifiering än ett system för biometrisk fjärridentifiering i realtid.

(39) *offentligt tillgänglig plats*: varje fysisk plats som är tillgänglig för allmänheten, utan hänsyn till om vissa villkor för tillträde kan vara tillämpliga.

(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,

(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 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) *nationell tillsynsmyndighet*: den myndighet som av en medlemsstat tilldelas ansvaret för genomförandet och tillämpningen av denna förordning, för samordningen av den verksamhet som anförtrotts den medlemsstaten, för att fungera som gemensam kontaktpunkt för kommissionen och för att företräda medlemsstaten i den europeiska nämnden för artificiell intelligens.

(43) *nationell behörig myndighet*: den nationella tillsynsmyndigheten, den anmälande myndigheten och marknadskontrollmyndigheten.

(44) *allvarlig incident*: en incident som direkt eller indirekt orsakar, kan ha orsakat eller skulle kunna orsaka något av följande:

(a) Dödsfall eller allvarlig skada för en persons hälsa, för egendom eller för miljön.

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

Artikel 4
Ändringar av bilaga I

Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 73 med avseende på att ändra förteckningen över de tekniker och metoder som förtecknas i bilaga I i syfte att uppdatera förteckningen så att den speglar marknadsutvecklingen och den tekniska utvecklingen på grundval av egenskaper som liknar de tekniker och metoder som förtecknas där.

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 för att väsentligt snedvrida en persons beteende på ett sätt som orsakar eller 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, som härrör från ålder eller fysisk eller psykisk funktionsnedsättning, hos en specifik grupp av personer, för att väsentligt snedvrida beteendet hos en person som tillhör den gruppen på ett sätt som orsakar eller 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 av offentliga myndigheter eller på deras vägnar för utvärdering eller klassificering av fysiska personers pålitlighet 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 hela 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 hela 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 för brottsbekämpningsändamål, såvida inte och endast i den mån sådan användning är absolut nödvändig för något av följande syften:

i) Målinriktad sökning efter specifika potentiella brottsoffer, inbegripet försvunna barn.

ii) Förhindrande av ett specifikt, betydande och överhängande hot mot fysiska personers liv eller fysiska säkerhet eller förhindrande av en terroristattack.

iii) Avslöjande, lokalisering, identifiering eller lagföring av en gärningsman eller misstänkt vid brott som avses i artikel 2.2 i rådets rambeslut 2002/584/RIF[62] och som i den berörda medlemsstaten kan leda till fängelsestraff eller annan frihetsberövande åtgärd för en maxperiod av minst tre år, i enlighet med 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.

(b) Konsekvenserna av användningen av systemet för alla berörda personers rättigheter och friheter, särskilt vad gäller hur allvarliga, sannolika och omfattande dessa konsekvenser är.

[62] 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).

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 enskild 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 och tillståndet får då begäras under eller efter användningen.

   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, 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. Oavsett om ett AI-system släpps ut på marknaden eller tas i bruk oberoende av de produkter som avses i leden a och b ska det AI-systemet betraktas som högrisksystem om båda följande villkor är uppfyllda:

   (a) AI-systemet är avsett att användas som en säkerhetskomponent i en produkt, eller är i sig en produkt, som omfattas av den unionslagstiftning om harmonisering som förtecknas i bilaga II.

(b) Den produkt vars säkerhetskomponent är AI-systemet, eller själva AI-systemet som en produkt, måste genomgå en tredjepartsbedömning av överensstämmelse för att den produkten ska kunna släppas ut på marknaden eller tas i bruk i enlighet med den unionslagstiftning om harmonisering som förtecknas i bilaga II.

2. Utöver de AI-system med hög risk som avses i punkt 1 ska AI-system som avses i bilaga III också betraktas som högrisksystem.

Artikel 7
Ändringar av bilaga III

1. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 73 med avseende på att uppdatera 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 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.

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.

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 bestå av en kontinuerlig iterativ process som löper under hela livscykeln för ett AI-system med hög risk, med krav på regelbunden och systematisk uppdatering. Det skall innehålla följande steg:

(a) Identifiering och analys av kända och förutsebara risker förbundna med varje AI-system med hög risk.

(b) Uppskattning och utvärdering av de risker som kan uppstå när AI-systemet med hög risk används i enlighet med dess avsedda ändamål och under förhållanden där det kan förekomma rimligen förutsebar felaktig användning.

(c) Utvärdering av andra risker som eventuellt kan uppstå på grundval av en analys av data som samlats in från det system för övervakning efter utsläppande på marknaden som avses i artikel 61.

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

3. I de riskhanteringsåtgärder som avses i punkt 2 d ska vederbörlig hänsyn tas till de effekter och möjliga interaktioner som följer av den kombinerade tillämpningen av kraven i detta kapitel 2. De ska ta hänsyn till den allmänt erkända bästa tekniken, inbegripet såsom den avspeglas i relevanta harmoniserade standarder eller gemensamma specifikationer.

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, förutsatt att AI-systemet med hög risk används i enlighet med sitt avsedda ändamål eller under förhållanden där det

kan förekomma rimligen förutsebar felaktig användning. Dessa kvarvarande risker ska meddelas användaren.

Vid fastställandet av de lämpligaste riskhanteringsåtgärderna ska följande säkerställas:

(a) Eliminering eller minskning av risker så långt som möjligt genom lämplig konstruktion och utveckling.

(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.

När risker i samband med användningen av AI-systemet med hög risk elimineras eller minskas 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 i syfte att identifiera de lämpligaste riskhanteringsåtgärderna. Testerna ska säkerställa att AI-system med hög risk fungerar konsekvent för sitt avsedda ändamål och att de uppfyller kraven i detta kapitel.

6. Testförfarandena ska vara lämpliga för att uppnå det avsedda ändamålet med AI-systemet och behöver inte gå utöver vad som är nödvändigt för att uppnå detta ändamål.

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. Vid genomförandet av det riskhanteringssystem som beskrivs i punkterna 1–7 ska särskild hänsyn tas till huruvida barn sannolikt kommer att ha tillgång till eller påverkas av AI-systemet med hög risk.

9. För kreditinstitut som regleras genom direktiv 2013/36/EU ska de aspekter som beskrivs i punkterna 1–8 ingå i de riskhanteringsförfaranden som dessa institut fastställer i enlighet med artikel 74 i det direktivet.

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) datainsamling,

(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,

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

3. Tränings-, validerings- och testningsdataset ska vara relevanta, representativa, 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. Lämpliga metoder för dataförvaltning och datahantering ska tillämpas för utvecklingen av andra AI-system med hög risk än sådana som använder teknik som inbegriper träning av modeller för att säkerställa att dessa AI-system med hög risk uppfyller punkt 2.

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 för att bedöma om AI-systemet uppfyller dessa krav. Den ska minst innehålla de delar som anges i bilaga IV.

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 utformas och utvecklas med funktioner som möjliggör automatisk registrering av händelser (loggar) medan AI-systemen med hög risk är i drift. Dessa loggningsfunktioner ska överensstämma med erkända standarder eller gemensamma specifikationer.

2. Loggningsfunktionerna ska säkerställa en spårbarhetsnivå som omfattar AI-systemets funktion under hela dess livscykel och som är lämplig för systemets avsedda ändamål.

3. Loggningsfunktionerna ska i synnerhet möjliggöra övervakning av driften av AI-systemet med hög risk med avseende på förekomsten av situationer som kan resultera i att AI-systemet utgör en risk i den mening som avses i artikel 65.1 eller leda till en väsentlig ändring, och ska underlätta den övervakning efter utsläppande på marknaden som avses i artikel 61.

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 för att användare ska kunna tolka systemets utdata och använda dem på lämpligt sätt. En lämplig typ och grad av transparens ska säkerställas, i syfte att uppnå uppfyllelse av användarens och leverantörens relevanta skyldigheter enligt kapitel 3 i denna avdelning.

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,

ii) den nivå avseende noggrannhet, robusthet och cybersäkerhet som avses i artikel 15 mot vilken AI-systemet med hög risk har testats och validerats och som kan förväntas, samt alla kända och förutsebara omständigheter som kan påverka den förväntade noggrannhets-, robusthets- och cybersäkerhetsnivån,

iii) varje känd eller förutsebar omständighet, som har samband med användningen av AI-systemet med hög risk i enlighet med dess avsedda ändamål eller under förhållanden där det kan förekomma rimligen förutsebar felaktig användning, som kan leda till risker för hälsa och säkerhet eller grundläggande rättigheter,

iv) dess prestanda vad gäller de 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-, valideringS- och testningsdataset som används, med beaktande av AI-systemets avsedda ändamål.

(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) Den förväntade livslängden för AI-systemet med hög risk och alla nödvändiga underhålls- och omsorgsåtgärder för att säkerställa att AI-systemet fungerar korrekt, även när det gäller programvaruuppdateringar.

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 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. De åtgärder som avses i punkt 3 ska göra det möjligt för de personer som fått i uppdrag att ombesörja mänsklig tillsyn att göra följande, beroende på omständigheterna:

   (a) Fullt ut förstå kapaciteten och begränsningarna hos AI-systemet med hög risk och på vederbörligt sätt kunna övervaka dess drift, så att tecken på avvikelser, funktionsstörningar och oväntad prestanda kan upptäckas och åtgärdas så snart som möjligt.

   (b) Förbli medvetna om den möjliga tendensen att automatiskt eller i alltför hög grad lita på de utdata som produceras av ett AI-system med hög risk (”automationssnedvridning”, ”automation bias”), särskilt när det gäller AI-system med hög risk som används för att tillhandahålla information eller rekommendationer för beslut som ska fattas av fysiska personer.

   (c) Korrekt kunna tolka utdata från AI-systemet med hög risk, särskilt med beaktande av systemets egenskaper och tillgängliga tolkningsverktyg och tolkningsmetoder.

   (d) I vissa situationer kunna 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) Kunna 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 av minst två fysiska personer.

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 man säkerställer att eventuellt snedvridna utdata, på grund av att utdata används som indata för framtida drift (”återföring”), 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,

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

(c) upprätta den tekniska dokumentationen för AI-systemet med hög risk,

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

(e) säkerställa att AI-systemet med hög risk genomgår det relevanta förfarandet för bedömning av överensstämmelse innan det släpps ut på marknaden eller tas i bruk,

(f) fullgöra de registreringsskyldigheter som avses i artikel 51,

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

(h) informera de nationella behöriga myndigheterna 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 allvarliga incidenter och av funktionsstörningar 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.

3. För leverantörer som är kreditinstitut som regleras av direktiv 2013/36/EU ska skyldigheten att införa ett kvalitetsstyrningssystem anses vara uppfylld genom att man följer reglerna om former för intern styrning, processer och metoder enligt artikel 74 i det direktivet. I detta sammanhang ska alla harmoniserade standarder som avses i artikel 40 i denna förordning beaktas.

Artikel 18
Skyldighet att upprätta teknisk dokumentation

1. Leverantörer av AI-system med hög risk ska upprätta den tekniska dokumentation som avses i artikel 11 i enlighet med bilaga IV.

2. Leverantörer som är kreditinstitut som regleras av direktiv 2013/36/EU ska underhålla den tekniska dokumentationen som en del av dokumentationen om intern styrning, styrformer, processer och metoder enligt artikel 74 i det direktivet.

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. När det gäller AI-system med hög risk som avses i punkt 5 b i bilaga III och som släpps ut på marknaden eller tas i bruk av leverantörer som är kreditinstitut som regleras av direktiv 2013/36/EU, ska bedömningen av överensstämmelse utföras som ett led i det förfarande som avses i artiklarna 97–101 i det direktivet.

Artikel 20
Automatiskt genererade loggar

1. Leverantörer av AI-system med hög risk ska spara de loggar 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. Loggarna ska sparas under en period som är lämplig mot bakgrund av det avsedda ändamålet med AI-systemet med hög risk och tillämpliga rättsliga skyldigheter enligt unionsrätten eller nationell rätt.

2. Leverantörer som är kreditinstitut som regleras av direktiv 2013/36/EU ska upprätthålla de loggar som genereras automatiskt av deras AI-system med hög risk som en del av dokumentationen enligt artikel 74 i det direktivet.

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 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 av den berörda medlemsstaten fastställt officiellt unionsspråk. På motiverad begäran av en nationell behörig myndighet ska leverantörer också ge den myndigheten tillgång till de loggar 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 24
Produkttillverkares skyldigheter

Om ett AI-system med hög risk som berör produkter som omfattas av de rättsakter som förtecknas i avsnitt A i bilaga II släpps ut på marknaden eller tas i bruk tillsammans med den produkt som tillverkas i enlighet med dessa rättsakter och under produkttillverkarens namn, ska produkttillverkaren ta ansvar för att AI-systemet överensstämmer med denna förordning och, när det gäller AI-systemet, ha samma skyldigheter som föreskrivs i denna förordning för leverantören.

Artikel 25
Ombud

1. Innan leverantörer etablerade utanför unionen tillhandahåller sina AI-system på unionsmarknaden ska de, i de fall då en importör inte kan identifieras, genom skriftlig fullmakt utse ett ombud som är etablerat i unionen.

2. Ombudet ska utföra de uppgifter som anges i fullmakten från leverantören. Fullmakten ska ge ombudet befogenhet att utföra följande uppgifter:

   (a) Hålla en kopia av EU-försäkran om överensstämmelse och den tekniska dokumentationen tillgänglig för de nationella behöriga myndigheterna och de nationella myndigheter som avses i artikel 63.7.

   (b) På motiverad begäran ge en nationell behörig myndighet all information och dokumentation 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 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 behöriga nationella myndigheter om eventuella åtgärder som dessa vidtar med avseende på AI-systemet med hög risk.

Artikel 26
Importörers skyldigheter

1. Innan importörer av AI-system med hög risk släpper ut ett sådant system på marknaden ska de säkerställa att

   (a) det tillämpliga förfarandet för bedömning av överensstämmelse 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 märkning om överensstämmelse och åtföljs av erforderlig dokumentation och bruksanvisning.

2. Om en importör anser eller har skäl att tro att ett AI-system med hög risk inte överensstämmer med denna förordning, får importören 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 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.

5. Importörer ska på motiverad begäran ge nationella behöriga myndigheter all information och dokumentation som är nödvändig 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, inbegripet tillgång till de loggar 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. De ska också samarbeta med dessa myndigheter om alla åtgärder som nationella behöriga myndigheter vidtar med avseende på det systemet.

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 erforderlig dokumentation och bruksanvisning och att leverantören och importören av systemet, beroende på vad som är tillämpligt, har uppfyllt skyldigheterna i denna förordning.

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 som är nödvändig för att visa att ett högrisksystem uppfyller kraven i kapitel 2 i denna avdelning. Distributörer ska också samarbeta med den nationella behöriga myndigheten om alla åtgärder som vidtas av den myndigheten.

Artikel 28

Skyldigheter för distributörer, importörer, användare eller annan tredje part

1. Varje distributör, importör, användare eller annan tredje part ska vid tillämpningen av denna förordning anses vara en leverantör och ska ha de skyldigheter som leverantören har enligt artikel 16, under någon av följande omständigheter:

   (a) De släpper ut ett AI-system med hög risk på marknaden eller tar ett sådant system i bruk under eget namn eller varumärke.

   (b) De ändrar det avsedda ändamålet för ett AI-system med hög risk som redan har släppts ut på marknaden eller tagits i bruk.

   (c) De gör en väsentlig ändring av AI-systemet med hög risk.

2. Om de omständigheter som avses i punkt 1 b 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.

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.

2. Skyldigheterna i punkt 1 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 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 eller en funktionsstörning i den mening som avses i artikel 62 och avbryta användningen av AI-systemet. Om användaren inte kan nå leverantören ska artikel 62 gälla i tillämpliga delar.

   För användare som är kreditinstitut som regleras av direktiv 2013/36/EU ska den övervakningsskyldighet som föreskrivs i första stycket anses vara uppfylld genom att man följer reglerna om former för intern styrning, processer och metoder enligt artikel 74 i det direktivet.

5. Användare av AI-system med hög risk ska spara de loggar som genereras automatiskt av systemet i fråga, i den mån sådana loggar står under deras kontroll. Loggarna ska sparas under en period som är lämplig mot bakgrund av det avsedda ändamålet med AI-systemet med hög risk och tillämpliga rättsliga skyldigheter enligt unionsrätten eller nationell rätt.

   Användare som är kreditinstitut som regleras av direktiv 2013/36/EU ska underhålla loggarna som en del av dokumentationen om intern styrning, styrformer, processer och metoder i enlighet med artikel 74 i det direktivet.

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.

KAPITEL 4

ANMÄLANDE MYNDIGHETER OCH ANMÄLDA ORGAN

Artikel 30
Anmälande myndigheter

1. Varje medlemsstat ska utse eller etablera 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 utse ett nationellt ackrediteringsorgan som avses i förordning (EG) nr 765/2008 till anmälande myndighet.

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.

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

8. Anmälande myndigheter ska se till att bedömningar av överensstämmelse utförs på ett proportionerligt sätt, så att man undviker onödiga bördor för leverantörer och så att anmälda organ utför sin verksamhet med vederbörlig hänsyn till ett företags storlek, den sektor inom vilken det är verksamt, dess struktur och det berörda AI-systemets komplexitet.

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-tekniker 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 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.

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 detta till kommissionen och de andra medlemsstaterna med hjälp av det elektroniska anmälningsverktyg som har utvecklats och förvaltas av kommissionen.

3. Anmälan ska innehålla detaljerade uppgifter om bedömningarna av överensstämmelse, modulen eller modulerna för bedömning av överensstämmelse och den berörda AI-tekniken.

4. Det organ som bedömer överensstämmelse får bedriva verksamhet som anmält organ endast om kommissionen eller de andra medlemsstaterna inte har gjort invändningar inom en månad från anmälan.

5. Den anmälande myndigheten ska underrätta kommissionen och de andra medlemsstaterna om alla relevanta ändringar av anmälan.

Artikel 33
Anmälda organ

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. 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 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 berörda medlemsstaten 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. Därför måste det anmälda organet, vid alla tidpunkter och vid varje förfarande för bedömning av överensstämmelse och för varje typ av AI med hög risk för vilken det har utsetts, ständigt har tillräcklig administrativ, teknisk 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. 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 kan utföra sina uppgifter avseende bedömning, utseende, anmälan, kontroll och övervakning och för att underlätta den bedömning som beskrivs i detta kapitel.

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 anmälda organen ska se till att den anmälande myndigheten har tillgång till de relevanta dokumenten rörande bedömningen av underentreprenörens eller dotterbolagets kvalifikationer och det arbete som dessa har utfört i enlighet med denna förordning.

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. Om en anmälande myndighet misstänker eller har informerats om att ett anmält organ inte längre uppfyller de krav som anges i artikel 33 eller att det underlåter att

fullgöra sina skyldigheter, ska den anmälande myndigheten utan dröjsmål undersöka frågan med största möjliga omsorg. I detta sammanhang ska den anmälande myndigheten underrätta det berörda anmälda organet om de invändningar som framförts och ge det möjlighet att lämna synpunkter. Om en anmälande myndighet drar slutsatsen att ett anmält organ inte längre uppfyller de krav som anges i artikel 33 eller att det underlåter att fullgöra sina skyldigheter, ska den anmälande myndigheten när så är lämpligt, beroende på hur allvarlig underlåtenheten att uppfylla kraven eller fullgöra skyldigheterna är, begränsa anmälan, tillfälligt återkalla den eller dra den tillbaka. Myndigheten ska också omedelbart informera kommissionen och de andra medlemsstaterna om detta.

2. I händelse av begränsning, tillfällig återkallelse eller tillbakadragande av anmälan, eller om det anmälda organet har upphört med verksamheten, ska den anmälande myndigheten vidta lämpliga åtgärder för att säkerställa att det anmälda organets dokumentation antingen tas över av ett annat anmält organ eller hålls tillgänglig för de ansvariga anmälande myndigheterna på deras begäran.

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.

4. Om kommissionen konstaterar att ett anmält organ inte uppfyller eller inte längre uppfyller kraven som fastställs i artikel 33 ska den anta ett motiverat beslut för att anmoda den anmälande medlemsstaten att vidta erforderliga korrigerande åtgärder, inbegripet att vid behov återta 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 de områden som omfattas av denna förordning se till att lämplig samordning och ett lämpligt samarbete införs mellan de anmälda organ som är verksamma i förfaranden för bedömning av överensstämmelse av AI-system i enlighet med denna förordning och att samordningen och samarbetet bedrivs på ett tillfredsställande sätt genom en sektorsspecifik grupp av anmälda organ.

2. Medlemsstaterna 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.

KAPITEL 5

STANDARDER, BEDÖMNING AV ÖVERENSSTÄMMELSE, INTYG, REGISTRERING

Artikel 40
Harmoniserade standarder

AI-system med hög risk 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 i den omfattning som standarderna omfattar dessa krav.

Artikel 41
Gemensamma specifikationer

1. Om sådana harmoniserade standarder som avses i artikel 40 inte finns eller om kommissionen anser att de relevanta harmoniserade standarderna är otillräckliga eller att det finns ett behov av att ta itu med specifika säkerhetsproblem eller frågor som rör de grundläggande rättigheterna, får kommissionen genom genomförandeakter anta gemensamma specifikationer med avseende på de krav som anges i kapitel 2 i denna avdelning. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 74.2.

2. Kommissionen ska när den utarbetar de gemensamma specifikationer som avses i punkt 1 samla in synpunkter från relevanta organ eller expertgrupper som inrättats enligt relevant sektorsspecifik unionsrätt.

3. AI-system med hög risk som överensstämmer med de gemensamma specifikationer som hänvisas till i punkt 1 ska förutsättas överensstämma med de krav som fastställs i kapitel 2 i denna avdelning i den omfattning som de gemensamma specifikationerna omfattar dessa krav.

4. Om leverantörer inte följer de gemensamma specifikationer som avses i punkt 1 ska de vederbörligen motivera att de har antagit tekniska lösningar som åtminstone är likvärdiga med dessa.

Artikel 42
Presumtion om överensstämmelse med vissa krav

1. Med beaktande av deras avsedda ändamål ska AI-system med hög risk som har tränats och testats på data som berör den specifika geografiska, beteendemässiga och funktionella miljö inom vilken de är avsedda att användas antas uppfylla kravet i artikel 10.4.

2. AI-system med hög risk som har certifierats, eller för vilka en försäkran om överensstämmelse har utfärdats inom ramen för en ordning för cybersäkerhet i enlighet med Europaparlamentets och rådets förordning (EU) 2019/881[63], och till

[63] 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).

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, följa 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.

   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 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. När det gäller AI-system med hög risk som avses i punkt 5 b i bilaga III och som släpps ut på marknaden eller tas i bruk av kreditinstitut som regleras av direktiv 2013/36/EU, ska bedömningen av överensstämmelse utföras som ett led i det förfarande som avses i artiklarna 97–101 i det direktivet.

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. AI-system med hög risk ska genomgå ett nytt förfarande för bedömning av överensstämmelse när de ändras väsentligt, oavsett om det ändrade systemet är avsett att distribueras vidare eller fortsätter att användas av den nuvarande användaren.

   När det gäller AI-system med hög risk som fortsätter att lära sig efter att det har släppts ut på marknaden eller tagits i bruk, ska sådana ändringar av AI-systemet med hög risk och dess prestanda som leverantören på förhand har fastställt vid tidpunkten för den inledande bedömningen av överensstämmelse och som är en del av den information som ingår i den tekniska dokumentation som avses i punkt 2 f i bilaga IV inte utgöra en väsentlig ändring.

5. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 73 i syfte att uppdatera bilagorna VI och VII för att introducera element av förfarandena för bedömning av överensstämmelse som blir nödvändiga 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 av unionens officiella språk som bestäms av den medlemsstat där det anmälda organet är etablerat eller på ett annat av unionens officiella språk som det anmälda organet godtar.

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.

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

Medlemsstaterna ska se till att det finns ett förfarande för överklagande av de anmälda organens beslut för de parter som har ett berättigat intresse i beslutet.

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 organen, som utför liknande bedömningar av överensstämmelse avseende samma AI-teknik, relevant information om frågor som rör negativa och, på begäran, positiva resultat av bedömningar av överensstämmelse.

Artikel 47
Undantag från förfarandena för bedömning av överensstämmelse

1. Genom undantag från artikel 43 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. Godkännandet ska gälla under en

begränsad tid, medan de nödvändiga förfarandena för bedömning av överensstämmelse genomförs, och ska upphöra att gälla när dessa förfaranden har slutförts. Dessa förfaranden ska slutföras utan onödigt dröjsmål.

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.

3. Godkännandet ska anses vara motiverat om ingen medlemsstat eller kommissionen har gjort någon invändning inom 15 kalenderdagar efter mottagandet av den information som avses i punkt 2 om ett godkännande utfärdat av en marknadskontrollmyndighet i en medlemsstat i enlighet med punkt 1.

4. Om en medlemsstat inom 15 kalenderdagar efter mottagandet av den anmälan som avses i punkt 2 gör en invändning mot ett godkännande som utfärdats av en marknadskontrollmyndighet i en annan medlemsstat, eller om kommissionen anser att godkännandet strider mot unionslagstiftningen, eller att medlemsstatens slutsats om systemets överensstämmelse som avses i punkt 2 är ogrundad, ska kommissionen utan dröjsmål inleda samråd med den berörda medlemsstaten; den eller de operatörer som berörs ska rådfrågas och ha möjlighet att framföra sina åsikter. Mot bakgrund av detta ska kommissionen besluta om tillståndet är motiverat eller inte. Kommissionen ska rikta sitt beslut till den berörda medlemsstaten och den eller de berörda operatörerna.

5. Om godkännandet anses omotiverat ska detta dras tillbaka av den berörda medlemsstatens marknadskontrollmyndighet.

6. På AI-system med hög risk som är avsedda att användas som säkerhetskomponenter i enheter, eller som själva är enheter, och som omfattas av förordning (EU) 2017/745 och förordning (EU) 2017/746, ska genom undantag från punkterna 1–5 också artikel 59 i förordning (EU) 2017/745 och artikel 54 i förordning (EU) 2017/746 tillämpas med avseende på undantaget från bedömningen av överensstämmelse med kraven i kapitel 2 i denna avdelning.

Artikel 48
EU-försäkran om överensstämmelse

1. Leverantören ska upprätta en skriftlig 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 ges 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 det eller de officiella unionsspråk som krävs av 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 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.

2. Den CE-märkning som avses i punkt 1 i denna artikel ska omfattas av de allmänna principer som fastställs i artikel 30 i förordning (EG) nr 765/2008.

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
Lagringstid för handlingar

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.

Artikel 51
Registrering

Innan ett AI-system med hög risk som avses i artikel 6.2 släpps ut på marknaden eller tas i bruk ska leverantören eller, i tillämpliga fall, den auktoriserade representanten registrera detta system i den EU-databas som avses i artikel 60.

AVDELNING IV

TRANSPARENSKRAV FÖR VISSA AI-SYSTEM

Artikel 52
Transparenskrav för 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 på grund av användningens omständigheter och sammanhang. Denna skyldighet ska inte gälla AI-system som enligt lag får upptäcka, förebygga, utreda och lagföra brott, såvida inte dessa system är tillgängliga för allmänheten för att anmäla ett brott.

2. Användare av system för känsloigenkänning eller 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.

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 det är nödvändigt för utövandet av den rätt till yttrandefrihet och den rätt som avser konstens och den vetenskapliga forskningens frihet i Europeiska unionens stadga om de grundläggande rättigheterna, och under förutsättning att lämpliga skyddsåtgärder vidtas för tredje parts rättigheter och friheter.

4. Punkterna 1, 2 och 3 ska inte påverka de krav och skyldigheter som anges i avdelning III i denna förordning.

AVDELNING V

ÅTGÄRDER TILL STÖD FÖR INNOVATION

Artikel 53
Regulatoriska sandlådor för AI

1. Regulatoriska sandlådor för AI som inrättats av en eller flera medlemsstaters behöriga myndigheter eller den europeiska datatillsynsmannen ska tillhandahålla en kontrollerad miljö som underlättar utveckling, testning och validering av innovativa AI-system under en begränsad tid innan de släpps ut på marknaden eller tas i bruk i enlighet med en särskild plan. Detta ska ske under direkt tillsyn och vägledning av de behöriga myndigheterna i syfte att säkerställa efterlevnad av kraven i denna förordning och, i tillämpliga fall, annan unionslagstiftning och medlemsstaternas lagstiftning som övervakas inom ramen för sandlådan.

2. Medlemsstaterna ska se till att i den mån de innovativa AI-systemen inbegriper behandling av personuppgifter eller på annat sätt faller inom tillsynsområdet för

andra nationella myndigheter eller behöriga myndigheter som tillhandahåller eller stöder åtkomst till data, ska de nationella dataskyddsmyndigheterna och dessa andra nationella myndigheter knytas till driften av den regulatoriska sandlådan för AI.

3. De regulatoriska sandlådorna för AI ska inte påverka de behöriga myndigheternas tillsynsbefogenheter eller korrigerande befogenheter. Alla betydande risker för hälsa och säkerhet och för grundläggande rättigheter som upptäcks under utvecklingen och testningen av sådana system ska leda till omedelbara kompenserande åtgärder och, om detta inte är möjligt, leda till att utvecklings- och testprocessen avbryts till dess att sådana kompenserande åtgärder äger rum.

4. Deltagare i den regulatoriska sandlådan för AI ska förbli ansvariga, enligt tillämplig unionslagstiftning och medlemsstaternas lagstiftning om ansvarsskyldighet, för skada som åsamkas tredje part till följd av de experiment som äger rum i sandlådan.

5. Behöriga myndigheter i medlemsstaterna som har inrättat regulatoriska sandlådor för AI ska samordna sin verksamhet och samarbeta inom ramen för den europeiska nämnden för artificiell intelligens. De ska lämna årliga rapporter till nämnden och kommissionen om resultaten av genomförandet av dessa ordningar, 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.

6. Regulatoriska sandlådors former och villkor, inbegripet kriterierna för stödberättigande och förfarandet för ansökan, urval, deltagande och utträde ur sandlådan, samt deltagarnas rättigheter och skyldigheter ska fastställas i genomförandeakter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 74.2.

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 ska personuppgifter som lagligen samlats in för andra ändamål behandlas i syfte att utveckla och testa vissa innovativa AI-system i sandlådan på följande villkor:

   (a) De innovativa AI-systemen ska utvecklas för att skydda ett betydande allmänintresse på ett eller flera av följande områden:

      i) Förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten, under överinseende och ansvar av den behöriga myndigheten. Behandlingen ska grundas på medlemsstaternas eller unionens lagstiftning.

      ii) Allmän säkerhet och folkhälsa, inbegripet förebyggande, bekämpning och behandling av sjukdomar.

      iii) Att på hög nivå skydda och förbättra miljöns kvalitet.

   (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 några allvarliga risker för de registrerades grundläggande rättigheter 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.

(f) Behandling av personuppgifter inom ramen för sandlådan får inte leda till åtgärder eller beslut som påverkar de registrerade.

(g) Alla personuppgifter som behandlas i sandlådan raderas när deltagandet i sandlådan har upphört eller personuppgifternas lagringstid har löpt ut.

(h) Loggarna över behandlingen av personuppgifter inom ramen för sandlådan sparas under hela deltagandet i sandlådan och ett år efter det att det har upphört, endast i syfte av att och endast så länge som det är nödvändigt för att fullgöra ansvarighets- och dokumentationsskyldigheterna enligt denna artikel eller enligt annan tillämpning lagstiftning i unionen eller medlemsstaterna.

(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.

2. Punkt 1 påverkar inte tillämpningen av unionslagstiftning eller medlemsstaternas lagstiftning som utesluter behandling i andra syften än de som uttryckligen anges i den lagstiftningen.

Artikel 55
Åtgärder för småskaliga leverantörer och användare

1. Medlemsstaterna ska vidta följande åtgärder:

(a) Ge småskaliga leverantörer och nystartade företag prioriterad åtkomst till de regulatoriska sandlådorna för AI, i den mån de uppfyller behörighetskraven.

(b) Anordna särskilda medvetandehöjande åtgärder om tillämpningen av denna förordning som är anpassade till behoven hos småskaliga leverantörer och användare.

(c) Där det är lämpligt, inrätta en särskild kanal för att kommunicera med småskaliga leverantörer och användare och andra innovatörer i syfte av att ge vägledning och svara på frågor om genomförandet av denna förordning.

2. De småskaliga leverantörernas särskilda intressen och behov ska beaktas när avgifterna för bedömning av överensstämmelse enligt artikel 43 fastställs, och avgifterna ska minskas i proportion till deras storlek och marknadsstorlek.

AVDELNING VI

STYRNING

KAPITEL 1

DEN EUROPEISKA NÄMNDEN FÖR ARTIFICIELL INTELLIGENS

Artikel 56
Inrättande av den europeiska nämnden för artificiell intelligens

1. En europeisk nämnd för artificiell intelligens (*nämnden*) inrättas.
2. Nämnden ska ge råd och stöd till kommissionen för att
   (a) bidra till ett effektivt samarbete mellan de nationella tillsynsmyndigheterna och kommissionen i frågor som omfattas av denna förordning,
   (b) samordna och bidra till vägledning och analys av kommissionen, de nationella tillsynsmyndigheterna och andra behöriga myndigheter när det gäller nya problem som uppstår på den inre marknaden med avseende på frågor som omfattas av denna förordning,
   (c) bistå de nationella tillsynsmyndigheterna och kommissionen med att säkerställa en konsekvent tillämpning av denna förordning.

Artikel 57
Nämndens uppbyggnad

1. Nämnden ska bestå av de nationella tillsynsmyndigheterna, som ska företrädas av chefen eller motsvarande högre tjänsteman vid den myndigheten, och Europeiska datatillsynsmannen. Andra nationella myndigheter får bjudas in till möten där frågor av relevans för dem diskuteras.
2. Nämnden ska anta sin arbetsordning med enkel majoritet av sina ledamöter efter godkännande från kommissionen. Arbetsordningen ska också innehålla de operativa aspekter som rör utförandet av nämndens uppgifter enligt förteckningen i artikel 58. Nämnden får inrätta arbetsgrupper när så är lämpligt i syfte att granska specifika frågor.
3. En företrädare för kommissionen ska vara ordförande i nämnden. Kommissionen ska vara sammankallande till mötena och förbereda dagordningen i enlighet med nämndens uppdrag enligt denna förordning och enligt nämndens arbetsordning. Kommissionen ska tillhandahålla administrativt och analytiskt stöd till nämndens verksamhet i enlighet med denna förordning.
4. Nämnden får bjuda in externa experter och observatörer för att delta i dessa möten och får hålla utbyten med berörda tredje parter för att informera om sin verksamhet i lämplig utsträckning. I detta syfte får kommissionen underlätta utbyten mellan nämnden och andra unionsorgan, unionskontor, unionsbyråer och rådgivande grupper.

Artikel 58
Nämndens uppgifter

När nämnden ger råd och stöd till kommissionen inom ramen för artikel 56.2 ska den särskilt

(a) samla in och utbyta sakkunskap och bästa praxis bland medlemsstaterna,

(b) bidra till enhetlig administrativ praxis i medlemsstaterna, inbegripet hur de regulatoriska sandlådor som avses i artikel 53 fungerar,

(c) utfärda yttranden, rekommendationer eller skriftliga bidrag i frågor som rör genomförandet av denna förordning, särskilt

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.

KAPITEL 2

NATIONELLA BEHÖRIGA MYNDIGHETER

Artikel 59
Utseende av nationella behöriga myndigheter

1. Nationella behöriga myndigheter ska inrättats eller utses av varje medlemsstat i syfte att säkerställa tillämpningen och genomförandet av denna förordning. Nationella behöriga myndigheter ska vara organiserade och fungera på ett sådant sätt att deras verksamhet är objektiv och opartisk.

2. Varje medlemsstat ska utse en nationell tillsynsmyndighet bland de nationella behöriga myndigheterna. Den nationella tillsynsmyndigheten ska fungera som anmälande myndighet och marknadskontrollmyndighet, såvida inte en medlemsstat har organisatoriska och administrativa skäl att utse mer än en myndighet.

3. Medlemsstaterna ska underrätta kommissionen om vilken eller vilka myndigheter de har utsett och, i tillämpliga fall, om skälen för att utse mer än en myndighet.

4. Medlemsstaterna ska se till att de nationella behöriga myndigheterna har tillräckliga ekonomiska resurser och personalresurser för att kunna fullgöra sina uppgifter enligt denna förordning. I synnerhet ska de nationella behöriga myndigheterna ha ett tillräckligt antal anställda till ständigt förfogande, vars kompetens och sakkunskap ska inbegripa en ingående förståelse av teknik för artificiell intelligens, data och databehandling, grundläggande rättigheter, hälso- och säkerhetsrisker och kunskap om befintliga standarder och rättsliga krav.

5. Medlemsstaterna ska årligen rapportera till kommissionen om situationen för de nationella behöriga myndigheternas ekonomiska 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 kan ge vägledning och råd om genomförandet av denna förordning, inbegripet till småskaliga leverantörer. 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 FRISTÅENDE AI-SYSTEM MED HÖG RISK

Artikel 60
EU-databas för fristående AI-system med hög risk

1. Kommissionen ska i samarbete med medlemsstaterna inrätta och upprätthålla en EU-databas som innehåller den information som avses i punkt 2 om AI-system med hög risk som avses i artikel 6.2 och som är registrerade i enlighet med artikel 51.

2. Leverantörerna ska föra in de uppgifter som förtecknas i bilaga VIII i EU-databasen. Kommissionen ska ge dem tekniskt och administrativt stöd.

3. Information i EU-databasen ska vara tillgänglig för allmänheten.

4. EU-databasen ska innehålla personuppgifter endast i den mån det är nödvändigt för insamling och behandling av information i enlighet med denna förordning. Denna information ska omfatta namnen på och kontaktuppgifter till fysiska personer som ansvarar för att registrera systemet och som har rättslig behörighet att företräda leverantören.

5. Kommissionen ska vara personuppgiftsansvarig för EU-databasen. Den ska också se till att leverantörerna får tillräckligt tekniskt och administrativt stöd.

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 typen av AI-teknik och riskerna med AI-systemet med hög risk.

2. Systemet för övervakning efter utsläppandet på marknaden ska aktivt och systematiskt samla in, dokumentera och analysera relevanta data tillhandahållna av användare eller insamlade via andra källor vad gäller hur AI-systemen med hög risk presterar under hela sin livstid, och göra det möjligt för leverantören att utvärdera AI-systemens fortlöpande överensstämmelse med kraven i avdelning III kapitel 2.

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, där ett system och en plan för övervakning efter utsläppandet på marknaden redan har inrättats enligt den lagstiftningen, ska de element som beskrivs i punkterna 1, 2 och 3 i lämpliga fall integreras i det systemet och den planen.

   Första stycket ska också tillämpas på AI-system med hög risk som avses i punkt 5 b i bilaga III och som släpps ut på marknaden eller tas i bruk av kreditinstitut som regleras av direktiv 2013/36/EU.

KAPITEL 2

INFORMATIONSDELNING OM INCIDENTER OCH FUNKTIONSSTÖRNINGAR

Artikel 62
Rapportering av allvarliga incidenter och funktionsstörningar

1. Leverantörer av AI-system med hög risk som släpps ut på unionsmarknaden ska rapportera alla allvarliga incidenter eller funktionsstörningar i dessa system som åsidosätter skyldigheter enligt unionsrätt avsedda att skydda de grundläggande rättigheterna till marknadskontrollmyndigheterna i de medlemsstater där incidenten eller åsidosättandet inträffade.

   En sådan underrättelse ska göras omedelbart efter det att leverantören har fastställt ett orsakssamband mellan AI-systemet och incidenten eller funktionsstörningen eller den rimliga sannolikheten att det finns ett sådant samband, och under alla omständigheter senast 15 dagar efter det att leverantörerna fått kännedom om den allvarliga incidenten eller funktionsstörningen.

2. Efter att ha mottagit en underrättelse om ett åsidosättande av skyldigheter enligt unionsrätt avsedda att skydda de grundläggande rättigheterna ska 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 b i bilaga III och som släpps ut på marknaden eller tas i bruk av leverantörer som är kreditinstitut reglerade av direktiv 2013/36/EU och 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 eller funktionsstörningar begränsas

till sådana som utgör ett åsidosättande av skyldigheter enligt unionsrätt avsedda att skydda de grundläggande rättigheterna.

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 i avdelning III kapitel 3 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. Den nationella tillsynsmyndigheten ska regelbundet rapportera resultaten av relevant marknadskontroll till kommissionen. Den nationella tillsynsmyndigheten ska utan dröjsmål rapportera till kommissionen och berörda nationella konkurrensmyndigheter all information som framkommit i samband med marknadskontrollen och som kan vara av potentiellt intresse för tillämpningen av unionens konkurrenslagstiftning.

3. För AI-system med hög risk som har koppling 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.

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 myndighet som enligt den lagstiftningen ansvarar för den finansiella tillsynen över dessa institut.

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

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.

Artikel 64
Tillgång till data och dokumentation

1. Inom ramen för sin verksamhet ska marknadskontrollmyndigheterna ges full tillgång till de dataset för utbildning, validering och testning som leverantören använder, inbegripet genom programmeringsgränssnitt (API) eller andra lämpliga tekniska medel och verktyg som möjliggör fjärråtkomst.

2. Om det är nödvändigt för att bedöma om AI-systemet med hög risk överensstämmer med kraven i avdelning III kapitel 2 och på motiverad begäran ska marknadskontrollmyndigheterna ges tillgång till AI-systemets källkod.

3. Nationella offentliga myndigheter eller organ som utövar tillsyn över eller verkställer efterlevnaden av skyldigheter enligt unionslagstiftning som skyddar grundläggande rättigheter 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 en förteckning på den nationella tillsynsmyndighetens webbplats. 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 skyddet av 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 skyddet av de grundläggande rättigheterna föreligger 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 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 rimlig tid som den fastställer i förhållande till typen av risk.

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 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 dröjsmål informera kommissionen och de andra medlemsstaterna om dessa åtgärder.

6. I den information som avses i punkt 5 ska alla tillgängliga data ingå, särskilt de data 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) AI-systemet 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.

7. Marknadskontrollmyndigheterna i andra medlemsstater än den som inledde förfarandet ska utan 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 information 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.

9. Marknadskontrollmyndigheterna i alla medlemsstater ska se till att lämpliga begränsande åtgärder, till exempel att produkten dras tillbaka från marknaden, vidtas utan dröjsmål i fråga om den produkt som berörs.

Artikel 66
Unionsförfarande för skyddsåtgärder

1. Om en medlemsstat inom tre månader efter mottagandet av den anmälan som avses i artikel 65.5 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 medlemsstaten och operatören eller operatörerna och ska utvärdera den nationella åtgärden. På grundval av utvärderingsresultaten ska kommissionen besluta om den nationella åtgärden är berättigad eller inte inom nio månader från den anmälan som avses i artikel 65.5 och meddela beslutet till den berörda medlemsstaten.

2. Om den nationella åtgärden anses vara berättigad, ska alla medlemsstater vidta de åtgärder som krävs för att säkerställa att det AI-system som inte uppfyller kraven dras tillbaka från deras marknader och underrätta kommissionen om detta. Om den nationella åtgärden anses omotiverad ska den medlemsstat som berörs återkalla åtgärden.

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 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 uppfyller kraven i denna förordning men ändå utgör en risk för personers hälsa och säkerhet, för efterlevnad av skyldigheter enligt unionsrätt eller nationell rätt avsedda att skydda de grundläggande rättigheterna eller för andra aspekter av skyddet av allmänintresset 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 inom en rimlig tid som medlemsstaten fastställer i förhållande till typen av risk.

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 dröjsmål inleda samråd med medlemsstaterna och den eller de berörda operatörerna 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 medlemsstaterna.

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:

   (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.

AVDELNING IX

UPPFÖRANDEKODER

Artikel 69
Uppförandekoder

1. Kommissionen och medlemsstaterna ska uppmuntra och underlätta utarbetandet av uppförandekoder som syftar till att främja frivillig tillämpning av kraven i avdelning III kapitel 2 på AI-system som inte är system med hög risk, på grundval av tekniska specifikationer och lösningar som är lämpliga för att säkerställa överensstämmelse med sådana krav mot bakgrund av systemens avsedda ändamål.

2. Kommissionen och nämnden ska uppmuntra och underlätta utarbetandet av uppförandekoder som syftar till att främja frivillig tillämpning på AI-system av krav som rör exempelvis miljömässig hållbarhet, 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.

3. Uppförandekoder kan 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. Uppförandekoder kan omfatta ett eller flera AI-system med beaktande av likheten mellan de berörda systemens avsedda ändamål.

4. Kommissionen och nämnden ska ta hänsyn till småskaliga leverantörers och nystartade företags särskilda intressen och behov när de uppmuntrar och underlättar utarbetandet av uppförandekoder.

AVDELNING X

KONFIDENTIALITET OCH SANKTIONER

Artikel 70
Konfidentialitet

1. De nationella behöriga myndigheter och anmälda organ som deltar i tillämpningen av denna förordning ska respektera konfidentialiteten för den information och de data som de erhåller när de utför sina uppgifter och sin verksamhet på ett sådant sätt att de särskilt skyddar följande:

   (a) Immateriella rättigheter och en fysisk eller juridisk persons konfidentiella affärsinformation eller företagshemligheter, inklusive källkod, utom i de fall som avses i artikel 5 i 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.

   (c) Integriteten i straffrättsliga eller administrativa förfaranden.

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 immigrations- eller asylmyndigheter, om ett sådant röjande skulle äventyra allmänna och nationella säkerhetsintressen.

   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 de anmälda organens rättigheter och skyldigheter när det gäller att utbyta information och utfärda varningar och inte heller de berörda personernas straffrättsliga skyldighet att lämna information enligt medlemsstaternas rättsordningar.

4. Kommissionen och medlemsstaterna får vid behov utbyta konfidentiell information med de tillsynsmyndigheter i tredjeländer med vilka de har slutit bilaterala eller multilaterala avtal om konfidentialitet som garanterar en tillräcklig nivå av konfidentialitet.

Artikel 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 småskaliga leverantörers och nystartade företags intressen och deras ekonomiska bärkraft.

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

3. Följande överträdelser 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:

   (a) Bristande efterlevnad av det förbud mot tillämpningar av artificiell intelligens som avses i artikel 5.

   (b) AI-systemets bristande efterlevnad av kraven i artikel 10.

4. 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 20 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 4 % av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

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.

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,

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

   (c) storleken på och marknadsandelen för den operatör som begått 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.

Artikel 72

Administrativa sanktionsavgifter för unionens institutioner, byråer och organ

1. Europeiska datatillsynsmannen kan 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. Följande överträdelser ska medföra administrativa sanktionsavgifter på upp till 500 000 EUR:

   (a) Bristande efterlevnad av det förbud mot tillämpningar av artificiell intelligens som avses i artikel 5.

   (b) AI-systemets bristande efterlevnad av kraven i artikel 10.

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 4, 7.1, 11.3, 43.5, 43.6 och 48.5 ska ges till kommissionen tills vidare från och med den [*dagen för ikraftträdandet av denna förordning*].

3. Den delegering av befogenhet som avses i artiklarna 4, 7.1, 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 4, 7.1, 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 vad gäller 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 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. Kommissionen ska bedöma behovet av att ändra förteckningen i bilaga III en gång per år efter det att denna förordning har trätt i kraft.

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 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 ska kommissionen utvärdera uppförandekodernas inverkan och effektivitet för att främja tillämpningen av kraven i avdelning III kapitel 2 och eventuellt andra ytterligare krav för AI-system som inte är AI-system med hög risk.

5. Vid tillämpning av punkterna 1–4 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 1 till 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 [*24 månader efter förordningens ikraftträdande*].

3. Genom undantag från punkt 2

   (a) ska avdelning III kapitel 4 och avdelning VI tillämpas från och med den [*tre 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*
Ordföranden	*Ordföranden*

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets beteckning

1.2. Berörda politikområden

1.3. Typ av förslag eller initiativ

1.4. Mål

1.4.1. Allmänt/allmänna mål

1.4.2. Specifikt/specifika mål

1.4.3. Verkan eller resultat som förväntas

1.4.4. Prestationsindikatorer

1.5. Motivering till förslaget eller initiativet

1.5.1. Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet

1.5.2. Mervärdet av en åtgärd på unionsnivå (som kan beror på flera faktorer, t.ex. samordningsfördelar, rättslig förutsägbarhet, ökad effektivitet eller komplementaritet). Med ”mervärdet av en åtgärd på unionsnivå” menas det värde en unionsinsats tillför som går utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.

1.5.3. Huvudsakliga erfarenheter från liknande försök eller åtgärder

1.5.4. Förenlighet med den fleråriga budgetramen och eventuella synergieffekter med andra relevanta instrument.

1.5.5 En bedömning av de olika finansieringsalternativ som finns att tillgå, inbegripet möjligheter till omfördelning

1.6. Tid under vilken åtgärden kommer att pågå respektive påverka resursanvändningen

1.7. Planerad metod för genomförandet

2. FÖRVALTNING

2.1. Bestämmelser om uppföljning och rapportering

2.2. Administrations- och kontrollsystem

2.2.1. Motivering av den genomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås

2.2.2. Uppgifter om identifierade risker och om det interna kontrollsystem som inrättats för att begränsa riskerna

2.2.3. Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)

2.3. Åtgärder för att förebygga bedrägeri och oegentligheter/oriktigheter

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

3.2. Förslagets beräknade budgetkonsekvenser för anslagen

3.2.1. Sammanfattning av beräknad inverkan på driftsanslagen

3.2.2. Beräknad output som finansieras med driftsanslag

3.2.3. Sammanfattning av beräknad inverkan på de administrativa anslagen

3.2.4. Förenlighet med den gällande fleråriga budgetramen

3.2.5. Bidrag från tredje part

3.3. Beräknad inverkan på inkomsterna

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets beteckning

Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter

1.2. Berörda politikområden

Kommunikationsnät, innehåll och teknik

Inre marknaden, industri, entreprenörskap samt små och medelstora företag

Budgetkonsekvenserna avser de nya uppgifter som anförtros kommissionen, inbegripet stödet till EU:s AI-nämnd.

Verksamhet: Att forma EU:s digitala framtid

1.3. Typ av förslag eller initiativ

X **Ny åtgärd**

☐ **Ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd**[64]

☐ **Befintlig åtgärd vars genomförande förlängs i tiden**

☐ **Tidigare åtgärd som omformas till eller ersätts av en ny**

1.4. Mål

1.4.1. Allmänt/allmänna mål

Det allmänna målet för insatsen är att säkerställa en väl fungerande inre marknad genom att skapa förutsättningar för utveckling och användning av tillförlitlig AI i unionen.

1.4.2. Specifikt/specifika mål

Specifikt mål nr 1

Fastställa krav som är specifika för AI-system och skyldigheter för alla deltagare i värdekedjan i syfte att säkerställa att AI-system som släpps ut på marknaden och används är säkra och respekterar befintlig lagstiftning om grundläggande rättigheter och unionens värden.

Specifikt mål nr 2

Säkerställa rättslig förutsägbarhet för att underlätta investeringar och innovation inom AI genom att klargöra vilka grundläggande krav, skyldigheter och förfaranden för överensstämmelse och efterlevnad som måste följas för att släppa ut eller använda ett AI-system på unionsmarknaden.

Specifikt mål nr 3

Förbättra styrningen och den faktiska efterlevnaden av befintlig lagstiftning gällande grundläggande rättigheter och säkerhetskrav som är tillämpliga på AI-system genom

[64] I den mening som avses i artikel 54.2 a och b i budgetförordningen.

att tillhandahålla nya befogenheter, resurser och tydliga regler för berörda myndigheter om förfaranden för bedömning av överensstämmelse och förfaranden för efterhandskontroll samt fördelningen av styrnings- och tillsynsuppgifter mellan nationell nivå och EU-nivå.

Specifikt mål nr 4

Underlätta utvecklingen av en inre marknad för lagliga, säkra och tillförlitliga AI-tillämpningar och förhindra marknadsfragmentering genom att vidta EU-åtgärder för att fastställa minimikrav för AI-system som ska släppas ut och användas på unionsmarknaden i enlighet med befintlig lagstiftning om grundläggande rättigheter och säkerhet.

1.4.3. Verkan eller resultat som förväntas

Beskriv den verkan som förslaget eller initiativet förväntas få på de mottagare eller den del av befolkningen som berörs.

AI-leverantörer bör gynnas av en minimal men tydlig uppsättning krav, vilket skapar rättslig förutsägbarhet och säkerställer tillträde till hela den inre marknaden.

AI-användare bör gynnas av en rättslig förutsägbarhet om att de AI-system med hög risk som de köper följer EU:s lagar och värderingar.

Konsumenterna bör gynnas genom en minskad risk för kränkningar av deras säkerhet eller grundläggande rättigheter.

1.4.4. Prestationsindikatorer

Ange vilka indikatorer som ska användas för att följa upp hur förslaget eller initiativet genomförs.

Indikator 1

Antal allvarliga incidenter eller AI-utförande som utgör en allvarlig incident eller en överträdelse av skyldigheterna i fråga om grundläggande rättigheter (halvårsvis) per tillämpningsområde och beräknat a) i absoluta tal, b) som andel använda tillämpningar och c) som andel berörda medborgare.

Indikator 2

a) Totala AI-investeringar i EU (årligen).

b) Totala AI-investeringar av medlemsstat (årligen).

c) Andel företag som använder AI (årligen).

d) Andel små och medelstora företag som använder AI (årligen).

a) och b) kommer att beräknas på grundval av officiella källor och jämföras med privata uppskattningar.

c) och d) kommer att samlas in genom regelbundna företagsundersökningar.

1.5. Motivering till förslaget eller initiativet

1.5.1. Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet

Förordningen bör tillämpas fullt ut ett och ett halvt år efter det att den har antagits. Delar av styrningsstrukturen bör dock finnas på plats före detta datum. Medlemsstaterna ska särskilt tidigare ha utsett befintliga myndigheter och/eller inrättat nya myndigheter som utför de uppgifter som anges i lagstiftningen, och EU:s AI-nämnd bör vara inrättad och verksam. När lagstiftningen börjar tillämpas bör den europeiska databasen över AI-system vara fullt operativ. Parallellt med antagandeprocessen är det därför nödvändigt att utveckla databasen så att den är färdigutvecklad när förordningen träder i kraft.

1.5.2. Mervärdet av en åtgärd på unionsnivå (som kan beror på flera faktorer, t.ex. samordningsfördelar, rättslig förutsägbarhet, ökad effektivitet eller komplementaritet). Med ”mervärdet av en åtgärd på unionsnivå” menas det värde en unionsinsats tillför som går utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.

Ett framväxande lapptäcke av potentiellt avvikande nationella regler kommer att hindra ett smidigt tillhandahållande av AI-system över hela EU och är ineffektivt när det gäller att säkerställa säkerheten och skyddet av de grundläggande rättigheterna och unionens värden i de olika medlemsstaterna. En gemensam EU-lagstiftning om AI skulle kunna främja den inre marknaden och har stor potential att ge den europeiska industrin en konkurrensfördel på den globala arenan och stordriftsfördelar som inte kan uppnås av enskilda medlemsstater på egen hand.

1.5.3. Huvudsakliga erfarenheter från liknande försök eller åtgärder

Direktiv 2000/31/EG om elektronisk handel utgör den centrala ramen för den inre marknadens funktion och för övervakningen av digitala tjänster och fastställer en grundläggande struktur för en allmän samarbetsmekanism mellan medlemsstaterna, som i princip omfattar alla krav som är tillämpliga på digitala tjänster. Utvärderingen av direktivet pekade på brister i flera aspekter av denna samarbetsmekanism, bland annat viktiga förfarandemässiga aspekter såsom avsaknaden av tydliga tidsramar för svar från medlemsstaterna i kombination med en allmän brist på lyhördhet för begäranden från deras motparter. Detta har under årens lopp lett till bristande förtroende mellan medlemsstaterna när det gäller att ta itu med frågor som gäller leverantörer som erbjuder digitala tjänster över gränserna. Utvärderingen av direktivet visade att det behövs en differentierad uppsättning regler och krav på EU-nivå. Därför skulle genomförandet av de särskilda skyldigheter som fastställs i denna förordning kräva en särskild samarbetsmekanism på EU-nivå, med en styrningsstruktur som säkerställer samordning av specifika ansvariga organ på EU-nivå.

1.5.4. Förenlighet med den fleråriga budgetramen och eventuella synergieffekter med andra relevanta instrument.

I förordningen om harmoniserade regler för artificiell intelligens och om ändring av vissa unionslagstiftningsakter fastställs en ny gemensam ram med krav som är tillämplig på AI-system, som sträcker sig långt utöver den ram som fastställs i befintlig lagstiftning. Därför måste en ny nationell och europeisk reglerings- och samordningsfunktion inrättas med detta förslag.

När det gäller möjliga synergier med andra lämpliga instrument kan rollen som anmälande myndighet på nationell nivå utövas av nationella myndigheter som utför liknande uppgifter inom ramen för andra EU-förordningar.

Genom att öka förtroendet för AI och på så sätt uppmuntra investeringar i utveckling och införande av AI kompletterar förordningen dessutom programmet för ett digitalt Europa, för vilket främjandet av spridningen av AI är en av fem prioriteringar.

1.5.5. En bedömning av de olika finansieringsalternativ som finns att tillgå, inbegripet möjligheter till omfördelning

Personalen kommer att omfördelas. Övriga kostnader kommer att stödjas genom anslaget för ett digitalt Europa eftersom målet för denna förordning – att säkerställa

tillförlitlig AI – direkt bidrar till ett centralt mål för ett digitalt Europa – att påskynda utvecklingen och användningen av AI i Europa.

1.6. Tid under vilken åtgärden kommer att pågå respektive påverka resursanvändningen

Förslag eller initiativ som pågår under ☐ **begränsad tid**

– ☐ Förslaget eller initiativet ska gälla från [den DD/MM]ÅÅÅÅ till [den DD/MM]ÅÅÅÅ.

– ☐ Budgetkonsekvenser från och med ÅÅÅÅ till och med ÅÅÅÅ för åtagandebemyndiganden och från och med ÅÅÅÅ till och med ÅÅÅÅ för betalningsbemyndiganden.

X Förslag eller initiativ som pågår under en **obegränsad tid**

– Efter en inledande period från ett till två år (bekräftas senare),

– beräknas genomförandetakten nå en stabil nivå.

1.7. Planerad metod för genomförandet[65]

X **Direkt förvaltning** som sköts av kommissionen

– ☐ inom dess tjänstegrenar, vilket också inbegriper personalen vid unionens delegationer

– ☐ av genomförandeorgan

☐ **Delad förvaltning** med medlemsstaterna

☐ **Indirekt förvaltning** genom delegering av budgetgenomförandet till

– ☐ tredjeländer eller organ som de har utsett

– ☐ internationella organisationer och organ kopplade till dem (ange vilka)

– ☐EIB och Europeiska investeringsfonden

– ☐ organ som avses i artiklarna 70 och 71 i budgetförordningen

– ☐ offentligrättsliga organ

– ☐ privaträttsliga organ som anförtrotts uppgifter som faller inom offentlig förvaltning och som lämnat tillräckliga ekonomiska garantier

– ☐ organ som omfattas av privaträtten i en medlemsstat, som anförtrotts genomförandet av ett offentlig-privat partnerskap och som lämnat tillräckliga ekonomiska garantier

– ☐ personer som anförtrotts ansvaret för genomförandet av särskilda åtgärder inom Gusp som följer av avdelning V i fördraget om Europeiska unionen och som anges i den grundläggande rättsakten

– *Vid fler än en metod, ange kompletterande uppgifter under ”Anmärkningar”.*

Anmärkningar

65 Närmare förklaringar av de olika metoderna för genomförande med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. FÖRVALTNING

2.1. Bestämmelser om uppföljning och rapportering

Ange intervall och andra villkor för sådana åtgärder

Förordningen kommer att ses över och utvärderas fem år efter förordningens ikraftträdande. Kommissionen kommer att rapportera resultaten av utvärderingen till Europaparlamentet, rådet och Europeiska ekonomiska och sociala kommittén.

2.2. Administrations- och kontrollsystem

2.2.1. Motivering av den genomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås

Genom förordningen införs en ny policy när det gäller harmoniserade regler för tillhandahållande av AI-system på den inre marknaden, samtidigt som säkerheten och de grundläggande rättigheterna respekteras. Dessa nya regler kräver en mekanism för enhetlighet vid gränsöverskridande tillämpning av skyldigheterna inom ramen för förordningen i form av en ny rådgivande grupp som samordnar de nationella myndigheternas verksamhet.

För att klara av dessa nya uppgifter är det nödvändigt att på lämpligt sätt förse kommissionens avdelningar med resurser. Genomförandet av den nya förordningen beräknas kräva 10 heltidsekvivalenter (5 heltidsekvivalenter för stöd till nämndens verksamhet och 5 heltidsekvivalenter för Europeiska datatillsynsmannen som fungerar som ett anmälande organ för AI-system som används av ett EU-organ).

2.2.2. Uppgifter om identifierade risker och om det interna kontrollsystem som inrättats för att begränsa riskerna

För att säkerställa att nämndens ledamöter har möjlighet att göra en välgrundad analys på grundval av faktaunderlag, föreskrivs det att nämnden bör stödjas av kommissionens administrativa struktur och att en expertgrupp inrättas för att vid behov tillhandahålla ytterligare sakkunskap.

2.2.3. Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)

Med tanke på det låga värdet per transaktion (t.ex. ersättning av resekostnader för en delegat för ett möte) förefaller standardkontrollförfarandena vara tillräckliga när det gäller möteskostnaderna. När det gäller utvecklingen av databasen har tilldelningen av kontrakt ett starkt internt kontrollsystem inom GD Kommunikationsnät, innehåll och teknik genom centraliserad upphandling.

2.3. Åtgärder för att förebygga bedrägeri och oegentligheter/oriktigheter

Beskriv förebyggande åtgärder (befintliga eller planerade), t.ex. från strategi för bedrägeribekämpning.

De befintliga bedrägeriförebyggande åtgärder som är tillämpliga på kommissionen kommer att täcka de ytterligare anslag som krävs för denna förordning.

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

- Befintliga budgetrubriker (även kallade ”budgetposter”)

Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd

Rubrik i den fleråriga budgetramen	Budgetrubrik	Typ av utgift	Bidrag			
	Antal	Diff./Icke-diff.[66]	från Efta-länder[67]	från kandidat-länder[68]	från tredje-länder	enligt artikel 21.2 b i budget-förordningen
7	20 02 06 Administrativa utgifter	Icke-diff	NEJ	NEJ	NEJ	NEJ
1	02 04 03 DEP Artificiell intelligens	Diff.	JA	NEJ	NEJ	NEJ
1	02 01 30 01 Stödutgifter för programmet för ett digitalt Europa	Icke-diff	JA	NEJ	NEJ	NEJ

3.2. Förslagets beräknade budgetkonsekvenser för anslagen

3.2.1. Sammanfattning av den beräknade inverkan på utgifterna för driftsanslag

– ☐ Förslaget/initiativet kräver inte att driftsanslag tas i anspråk

– X Förslaget/initiativet kräver att driftsanslag tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

Rubrik i den fleråriga	1	

[66] Differentierade respektive icke-differentierade anslag.
[67] Efta: Europeiska frihandelssammanslutningen.
[68] Kandidatländer och i förekommande fall potentiella kandidatländer i västra Balkan.

budgetramen		

GD: Kommunikationsnät, innehåll och teknik				År **2022**	År **2023**	År **2024**	År **2025**	År **2026**	År **2027**[69]	**TOTALT**	
• Driftsanslag											
Budgetpost[70] 02 04 03		Åtaganden	(1 a)		1,000						**1,000**
		Betalningar	(2a)		0,600	0,100	0,100	0,100	0,100		**1,000**
Budgetrubrik		Åtaganden	(1b)								
		Betalningar	(2b)								
Anslag av administrativ natur som finansieras genom ramanslagen för vissa operativa program[71]											
Budgetpost 02 01 30 01			(3)		0,240	0,240	0,240	0,240	0,240		**1,200**
TOTALA anslag för GD Kommunikationsnät, innehåll och teknik		Åtaganden	=1a+1b +3		**1,240**		**0,240**	**0,240**	**0,240**		**2,200**
		Betalningar	=2a+2b +3		**0,840**	**0,340**	**0,340**	**0,340**	**0,340**		**2,200**

• TOTALA driftsanslag	Åtaganden	(4)		1,000						**1,000**

69 Vägledande och beroende av tillgängliga budgetmedel.

70 Enligt den officiella kontoplanen.

71 Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

	Betalningar	(5)		0,600	0,100	0,100	0,100	0,100		**1,000**
• TOTALA anslag av administrativ natur som finansieras genom ramanslagen för vissa operativa program		(6)		**0,240**	**0,240**	**0,240**	**0,240**	**0,240**		**1,200**
TOTALA anslag för RUBRIK 1 i den fleråriga budgetramen	Åtaganden	=4+ 6		1,240	0,240	0,240	0,240	0,240		**2,200**
	Betalningar	=5+ 6		0,840	0,340	0,340	0,340	0,340		**2,200**

Om mer än en rubrik påverkas av förslaget/initiativet ska avsnittet ovan upprepas:

• Totala driftsanslag (alla rubriker avseende driftsanslag)	Åtaganden	(4)								
	Betalningar	(5)								
• TOTALA anslag av administrativ natur som finansieras genom ramanslagen för vissa operativa program (alla rubriker avseende driftsanslag)		(6)								
TOTALA anslag för RUBRIKERNA 1–6 i den fleråriga budgetramen (referensbelopp)	Åtaganden	=4+ 6								
	Betalningar	=5+ 6								

Rubrik i den fleråriga budgetramen	7	”Administrativa utgifter”

Detta avsnitt ska fyllas i med hjälp av det datablad för budgetuppgifter av administrativ natur som först ska föras in i bilagan till finansieringsöversikt för rättsakt (bilaga V till de interna reglerna), vilken ska laddas upp i DECIDE som underlag för samråden mellan kommissionens avdelningar.

Miljoner euro (avrundat till tre decimaler)

		År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	**Efter 2027**[72]	**TOTALT**
GD: Kommunikationsnät, innehåll och teknik								
• Personalresurser		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Övriga administrativa utgifter		**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,050**
TOTALT GD KOMMUNIKATIONSNÄT, INNEHÅLL OCH TEKNIK	**Anslag**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,850**
Europeiska datatillsynsmannen								
• Personalresurser		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Övriga administrativa utgifter								
TOTALT EUROPEISKA DATATILLSYNSMANNEN	**Anslag**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,800**
TOTALA anslag för RUBRIK 7 i den fleråriga budgetramen	(summa åtaganden = summa betalningar)	1,530	1,530	1,530	1,530	1,530	1,530	**7,650**

Miljoner euro (avrundat till tre decimaler)

	År	År	År	År	År **2026**	År **2027**		**TOTALT**

[72] Alla belopp i denna kolumn är preliminära och under förutsättning att programmen fortsätter och att anslag finns tillgängliga.

		2022	2023	2024	2025				
TOTALA anslag för RUBRIKERNA 1–7 i den fleråriga budgetramen	Åtaganden		2,770	1,770	1,770	1,770	1,770		**9,850**
	Betalningar		2,370	1,870	1,870	1,870	1,870		**9,850**

3.2.2. Beräknad output som finansieras med driftsanslag

Åtagandebemyndiganden i miljoner euro (avrundat till tre decimaler)

Mål- och resultatbeteckning ⇩			År **2022**		År **2023**		År **2024**		År **2025**		År **2026**		År **2027**		Efter **2027**[73]		**TOTALT**	
	RESULTAT																	
	Typ	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 1[74]…																		
Databas					1	1,000	1		1		1		1		1	0,100	1	1,000
Möten – Resultat					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Kommunikationsverksamhet					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Delsumma för specifikt mål nr 1																		
SPECIFIKT MÅL nr 2…																		
- Resultat																		
Delsumma för specifikt mål nr 2																		
TOTALT					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

[73] Alla belopp i denna kolumn är preliminära och under förutsättning att programmen fortsätter och att anslag finns tillgängliga.

[74] Mål som redovisats under punkt 1.4.2 ”Specifikt/specifika mål…”.

3.2.3. Sammanfattning av beräknad inverkan på de administrativa anslagen

– ☐ Förslaget/initiativet kräver inte att anslag av administrativ natur tas i anspråk

– X Förslaget/initiativet kräver att anslag av administrativ natur tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

	År **2022**	År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	**Årligen efter 2027**[75]	**TOTALT**
RUBRIK 7 i den fleråriga budgetramen								
Personalresurser		1,520	1,520	1,520	1,520	1,520	**1,520**	**7,600**
Övriga administrativa utgifter		0,010	0,010	0,010	0,010	0,010	**0,010**	**0,050**
Delsumma RUBRIK 7 i den fleråriga budgetramen		1,530	1,530	1,530	1,530	1,530	**1,530**	**7,650**
Utanför RUBRIK 7[76] **i den fleråriga budgetramen**								
Personalresurser								
Andra utgifter av administrativ karaktär		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
Delsumma utanför RUBRIK 7 i den fleråriga budgetramen		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
TOTALT		**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**8,850**

Personalbehov och andra administrativa kostnader ska täckas genom anslag inom generaldirektoratet som redan har avdelats för att förvalta åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

75 Alla belopp i denna kolumn är preliminära och under förutsättning att programmen fortsätter och att anslag finns tillgängliga.

76 Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

3.2.3.1. Beräknat personalbehov

– ☐ Förslaget/initiativet kräver inte att personalresurser tas i anspråk

– X Förslaget/initiativet kräver att personalresurser tas i anspråk enligt följande:

Beräkningarna ska anges i heltidsekvivalenter

.		År **2023**	År **2024**	År **2025**	**2026**	**2027**	**Efter 2027**[77]	
• Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)								
20 01 02 01 (vid huvudkontoret eller vid kommissionens kontor i medlemsstaterna)		10	10	10	10	10	10	
20 01 02 03 (vid delegationer)								
01 01 01 01 (indirekta forskningsåtgärder)								
01 01 01 11 (direkta forskningsåtgärder)								
Annan budgetrubrik (ange vilken)								
• Extern personal (i heltidsekvivalenter) [78]								
20 02 01 (kontraktsanställda, nationella experter och vikarier finansierade genom ramanslaget)								
20 02 03 (kontraktsanställda, lokalanställda, nationella experter, vikarier och unga experter som tjänstgör vid delegationerna)								
XX 01 xx **yy zz** [79]	- vid huvudkontoret							
	- vid delegationer							
01 01 01 02 (kontraktsanställda, vikarier och nationella experter som arbetar med indirekta forskningsåtgärder)								
01 01 01 12 (kontraktsanställda, vikarier och nationella experter som arbetar med direkta forskningsåtgärder)								
Annan budgetrubrik (ange vilken)								
TOTALT		**10**	**10**	**10**	**10**	**10**	**10**	

XX motsvarar det politikområde eller den avdelning i budgeten som avses.

Personalbehoven ska täckas med personal inom generaldirektoratet som redan har avdelats för att förvalta åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

Datatillsynsmannen förväntas tillhandahålla hälften av de resurser som krävs.

Beskrivning av arbetsuppgifter:

Tjänstemän och tillfälligt anställda	För att förbereda totalt 13–16 möten, utarbeta rapporter, fortsätta policyarbetet, t.ex. när det gäller framtida ändringar av förteckningen över AI-tillämpningar med hög risk, och upprätthålla förbindelserna med medlemsstaternas myndigheter kommer det att krävas fyra heltidsekvivalenter AD och 1 heltidsekvivalent AST. För AI-system som utvecklats av EU-institutionerna ansvarar Europeiska datatillsynsmannen. På grundval av tidigare erfarenheter kan det uppskattas att 5 heltidsekvivalenter AD krävs för att uppfylla Europeiska datatillsynsmannens ansvar

[77] Alla belopp i denna kolumn är preliminära och under förutsättning att programmen fortsätter och att anslag finns tillgängliga.

[78] [Denna fotnot förklarar vissa initialförkortningar som inte används i den svenska versionen].

[79] Särskilt tak för finansiering av extern personal genom driftsanslag (tidigare s.k. BA-poster).

	enligt lagförslaget.
Extern personal	

3.2.4. Förenlighet med den gällande fleråriga budgetramen

– X Förslaget/initiativet kan finansieras fullständigt genom omfördelningar inom den berörda rubriken i den fleråriga budgetramen.

Ingen omplanering behövs.

– ☐ Förslaget/initiativet kräver användning av den outnyttjade marginalen under den relevanta rubriken i den fleråriga budgetramen och/eller användning av de särskilda instrumenten enligt definitionen i förordningen om den fleråriga budgetramen.

Beskriv vad som krävs, ange berörda rubriker och budgetrubriker, motsvarande belopp och de instrument som är föreslagna för användning.

– ☐ Förslaget/initiativet kräver en översyn av den fleråriga budgetramen.

Beskriv behovet av sådana åtgärder, och ange berörda rubriker i budgetramen, budgetrubriker i den årliga budgeten samt belopp.

3.2.5. Bidrag från tredje part

– X Det ingår inga bidrag från tredje part i det aktuella förslaget eller initiativet

– ☐ Förslaget eller initiativet kommer att medfinansieras enligt följande:

Anslag i miljoner euro (avrundat till tre decimaler)

	År **n**[80]	År **n+1**	År **n+2**	År **n+3**	För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)			Totalt
Ange vilken extern organisation eller annan källa som bidrar till finansieringen								
TOTALA anslag som tillförs genom medfinansiering								

[80] Med år n avses det år då förslaget eller initiativet ska börja genomföras. Ersätt ”n” med det förväntade första genomförandeåret (till exempel 2021). Samma sak gäller för följande år.

3.3. Beräknad inverkan på inkomsterna

– ☐ Förslaget/initiativet påverkar inkomsterna på följande sätt:

– ☐ Förslaget/initiativet påverkar inkomsterna på följande sätt:

– ☐ Påverkan på andra inkomster

– ☐ Påverkan på andra inkomster

– Ange om inkomsterna har avsatts för utgiftsposter ☐

Miljoner euro (avrundat till tre decimaler)

Budgetrubrik i den årliga budgetens inkomstdel:	Belopp som förts in för det innevarande budgetåret	Förslagets eller initiativets inverkan på inkomsterna[81]						
		År **n**	År **n+1**	År **n+2**	År **n+3**	För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)		
Artikel …….								

För inkomster avsatta för särskilda ändamål, ange vilka budgetrubriker i utgiftsdelen som berörs.

Övriga anmärkningar (till exempel vilken metod/formel som har använts för att beräkna effekten på inkomsterna eller någon annan information).

[81] När det gäller traditionella egna medel (tullar och sockeravgifter) ska nettobeloppen anges, dvs. bruttobeloppen minus 20 % avdrag för uppbördskostnader.