



Rådet for  
Den Europæiske Union

Bruxelles, den 23. april 2021  
(OR. en)

8115/21

---

**Interinstitutionel sag:  
2021/0106(COD)**

---

**TELECOM 156  
JAI 429  
COPEN 191  
CYBER 108  
DATAPROTECT 103  
EJUSTICE 41  
COSI 69  
IXIM 74  
ENFOPOL 148  
FREMP 103  
RELEX 347  
MI 271  
COMPET 275  
IA 60  
CODEC 573**

#### **FØLGESKRIVELSE**

---

fra:	Martine DEPREZ, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget:	22. april 2021
til:	Jeppe TRANHOLM-MIKKELSEN, generalsekretær for Rådet for Den Europæiske Union

---

Komm. dok. nr.:	COM(2021) 206 final
-----------------	---------------------

---

Vedr.:	Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING OM HARMONISEREDE REGLER FOR KUNSTIG INTELLIGENS (RETSAKTEN OM KUNSTIG INTELLIGENS) OG OM ÆNDRING AF VISSE AF UNIONENS LOVGIVNINGSMÆSSIGE RETSAKTER
--------	---

---

Hermed følger til delegationerne dokument COM(2021) 206 final.

---

Bilag: COM(2021) 206 final



EUROPA-  
KOMMISSIONEN

Bruxelles, den 21.4.2021  
COM(2021) 206 final

2021/0106 (COD)

Forslag til

**EUROPA-PARLAMENTETS OG RÅDETS FORORDNING**

**OM HARMONISEREDE REGLER FOR KUNSTIG INTELLIGENS (RETSAKTEN  
OM KUNSTIG INTELLIGENS) OG OM ÆNDRING AF VISSE AF UNIONENS  
LOVGIVNINGSMÆSSIGE RETSAKTER**

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

## **BEGRUNDELSE**

### **1. BAGGRUND FOR FORSLAGET**

#### **1.1. Forslagets begrundelse og formål**

Denne begrundelse ledsager forslaget til forordning om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens). Kunstig intelligens (AI) er en vifte af teknologier i hurtig udvikling, som kan medføre brede økonomiske og samfundsmæssige fordele på tværs af hele spektret af industrier og sociale aktiviteter. Ved at forbedre prognoser, optimere drift og ressourceallokering og personalisere leveringen af tjenester kan anvendelsen af kunstig intelligens fremme sociale og miljømæssige fremskridt og give virksomhederne og den europæiske økonomi afgørende konkurrencemæssige fordele. Der er især behov for en sådan indsats inden for vigtige sektorer, herunder klimaændringer, miljø og sundhed, den offentlige sektor, finans, mobilitet, indre anliggender og landbrug. De samme elementer og teknikker, der skaber de socioøkonomiske fordele ved kunstig intelligens, kan imidlertid også medføre nye risici eller negative konsekvenser for enkeltpersoner eller samfundet. I lyset af den hurtige teknologiske udvikling og de mulige udfordringer er EU fast besluttet på at stræbe efter en afbalanceret tilgang. Det er i Unionens interesse at bevare EU's teknologiske førerposition og sikre, at europæerne kan drage fordel af nye teknologier, der udvikles og som fungerer i overensstemmelse med Unionens værdier, grundlæggende rettigheder og principper.

Dette forslag lever op til det politiske tilsagn fra kommissionsformand Ursula von der Leyen, som i sine politiske retningslinjer for Kommissionen for 2019-2024 "En mere ambitiøs Union"<sup>1</sup> bebudede, at Kommissionen ville fremsætte forslag til lovgivning om en koordineret europæisk tilgang til de menneskelige og etiske konsekvenser af kunstig intelligens. I forlængelse heraf offentliggjorde Kommissionen den 19. februar 2020 "Hvidbog om kunstig intelligens – en europæisk tilgang til ekspertise og tillid"<sup>2</sup>. Hvidbogen indeholder politiske valgmuligheder, der har til formål både at fremme anvendelsen af kunstig intelligens og at håndtere de risici, der er forbundet med visse anvendelser af denne teknologi. Sigtet med dette forslag er at gennemføre den anden målsætning om udvikling af et tillidsmiljø ved at foreslå en retlig ramme for pålidelig kunstig intelligens. Forslaget er baseret på EU's værdier og grundlæggende rettigheder og har til formål at give brugere og befolkningen i bred forstand tillid til at anvende AI-baserede løsninger, samtidig med at virksomhederne tilskyndes til at udvikle dem. Kunstig intelligens bør være et redskab, der tjener mennesker og udgør en positiv kraft i samfundet med det endelige mål at øge menneskers velfærd. Regler for kunstig intelligens, der vedrører EU-markedet eller på anden måde påvirker mennesker i Unionen, bør derfor være menneskecentrerede, således at folk kan have tillid til, at teknologien anvendes på en måde, der er sikker og i overensstemmelse med lovgivningen, herunder respekten for de grundlæggende rettigheder. Efter offentliggørelsen af hvidbogen iværksatte Kommissionen en bred interessenthøring, som blev mødt med stor interesse af en lang række interessenter, som i vid udstrækning støttede regulerende indgreb til imødegåelse af de udfordringer og bekymringer, som den stigende brug af kunstig intelligens giver anledning til.

Med forslaget imødekommes også eksplicitte anmodninger fra Europa-Parlamentet og Det Europæiske Råd, som gentagne gange har opfordret til lovgivningsmæssige tiltag for at sikre et velfungerende indre marked for kunstig intelligens-systemer ("AI-systemer"), hvor både

---

<sup>1</sup> [https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission\\_da.pdf](https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_da.pdf)

<sup>2</sup> Europa-Kommissionen, Hvidbog om kunstig intelligens - en europæisk tilgang til ekspertise og tillid (COM (2020) 65 final).

fordele og risici ved kunstig intelligens håndteres tilfredsstillende på EU-plan. Hermed støttes målet om, at Unionen skal være førende på verdensplan inden for udvikling af sikker, pålidelig og etisk kunstig intelligens som anført af Det Europæiske Råd<sup>3</sup>, og der sikres beskyttelse af etiske principper, som Europa-Parlamentet specifikt har anmodet om<sup>4</sup>.

I 2017 opfordrede Det Europæiske Råd til "en erkendelse af, at det haster med at se nærmere på nye tendenser", herunder "spørgsmål som kunstig intelligens ..., samtidig med at der sikres et højt niveau af databeskyttelse, digitale rettigheder og etiske standarder."<sup>5</sup> I sine konklusioner fra 2019 om den koordinerede plan for udviklingen og anvendelsen af kunstig intelligens produceret i Europa<sup>6</sup> fremhævede Rådet endvidere betydningen af at sikre, at de europæiske borgeres rettigheder respekteres fuldt ud, og opfordrede til en revision af den relevante lovgivning for at gøre den egnet til formålet med de nye muligheder og udfordringer, der skyldes kunstig intelligens. Det Europæiske Råd har også opfordret til en klar definition af de AI-anvendelser, der bør betragtes som højrisiko-anvendelser<sup>7</sup>.

I de seneste konklusioner af 21. oktober 2020 opfordres der endvidere til at tackle visse AI-systemers uigennemsigthed, kompleksitet, forudindtagethed, en vis grad af uforudsigelighed og delvis autonome adfærd for at sikre, at de er forenelige med de grundlæggende rettigheder og for at lette håndhævelsen af retsfor skrifter<sup>8</sup>.

Europa-Parlamentet har også ydet en betydelig indsats i forbindelse med kunstig intelligens. I oktober 2020 vedtog det en række beslutninger vedrørende kunstig intelligens, herunder om etik<sup>9</sup>, ansvar<sup>10</sup> og ophavsret<sup>11</sup>. I 2021 blev disse efterfulgt af resolutioner om brugen af kunstig intelligens i straffesager<sup>12</sup> og inden for uddannelse, kultur og den audiovisuelle sektor<sup>13</sup>. Europa-Parlamentets beslutning om en ramme for etiske aspekter af kunstig intelligens, robotteknologi og relaterede teknologier anbefaler specifikt Kommissionen at foreslå lovgivningsmæssige tiltag for at udnytte mulighederne og fordelene ved kunstig intelligens, men også for at sikre beskyttelse af etiske principper. Beslutningen indeholder en tekst til det lovgivningsmæssige forslag til en forordning om etiske principper for udvikling,

---

<sup>3</sup> Det Europæiske Råd, [Ekstraordinært møde i Det Europæiske Råd \(1. og 2. oktober 2020\) – Konklusioner](#), EUCO 13/20, 2020, s. 6.

<sup>4</sup> Europa-Parlamentets beslutning af 20. oktober 2020 med henstillinger til Kommissionen om en ramme for etiske aspekter af kunstig intelligens, robotteknologi og relaterede teknologier, 2020/2012(INL).

<sup>5</sup> Det Europæiske Råd, [Møde i Det Europæiske Råd \(19. oktober 2017\) – Konklusioner](#), EUCO 14/17, 2017, s. 8.

<sup>6</sup> Rådet for Den Europæiske Union, [Kunstig intelligens b\) Konklusioner om en koordineret plan for kunstig intelligens - Vedtagelse](#) 6177/19, 2019.

<sup>7</sup> Det Europæiske Råd, [Ekstraordinært møde i Det Europæiske Råd \(1. og 2. oktober 2020\) – Konklusioner](#), EUCO 13/20, 2020.

<sup>8</sup> Rådet for Den Europæiske Union, [Formandskabets konklusioner – Chartret om grundlæggende rettigheder i forbindelse med kunstig intelligens og digital forandring](#), 11481/20, 2020.

<sup>9</sup> Europa-Parlamentets beslutning af 20. oktober 2020 med henstillinger til Kommissionen om en ramme for etiske aspekter af kunstig intelligens, robotteknologi og relaterede teknologier, [2020/2012\(INL\)](#).

<sup>10</sup> Europa-Parlamentets beslutning af 20. oktober 2020 med henstillinger til Kommissionen om en civilretlig erstatningsansvarsordning for kunstig intelligens, [2020/2014\(INL\)](#).

<sup>11</sup> Europa-Parlamentets beslutning af 20. oktober 2020 om intellektuel ejendomsret i forbindelse med udvikling af teknologier vedrørende kunstig intelligens, [2020/2015\(INI\)](#).

<sup>12</sup> Europa-Parlamentet. Udkast til betænkning om kunstig intelligens inden for strafferet og politiets og de retlige myndigheders anvendelse heraf i strafferetlige sager, [2020/2016\(INI\)](#).

<sup>13</sup> Europa-Parlamentet. Udkast til betænkning om kunstig intelligens inden for uddannelse, kultur og den audiovisuelle sektor [2020/2017\(INI\)](#). I den forbindelse har Kommissionen vedtaget [handlingsplanen for digital uddannelse 2021-2027: Omstilling af uddannelsessystemerne med henblik på den digitale tidsalder, som forudsætter udviklingen af etiske retningslinjer for AI og anvendelsen af data i undervisning — COM\(2020\) 624 final](#).

udbredelse og anvendelse af kunstig intelligens, robotteknologi og relaterede teknologier. I overensstemmelse med det politiske tilsagn, som kommissionsformand Ursula von der Leyen gav i sine politiske retningslinjer for så vidt angår beslutninger vedtaget af Europa-Parlamentet i henhold til artikel 225 i TEUF, tager dette forslag hensyn til Europa-Parlamentets ovennævnte beslutning i fuld overensstemmelse med proportionalitetsprincippet, nærhedsprincippet og princippet om bedre lovgivning.

På denne politiske baggrund fremlægger Kommissionen den foreslåede lovgivningsmæssige ramme for kunstig intelligens med følgende **specifikke mål**:

- at sørge for, at AI-systemer, der bringes i omsætning og anvendes på EU-markedet, er sikre og i overensstemmelse med eksisterende lovgivning om grundlæggende rettigheder og Unionens værdier
- at sikre retssikkerheden med henblik på at fremme investering og innovation inden for kunstig intelligens
- at forbedre forvaltning og effektiv håndhævelse af den eksisterende lovgivning om grundlæggende rettigheder og sikkerhedskrav til AI-systemer
- at fremme udviklingen af et indre marked for lovlige, sikre og pålidelige AI-anvendelser og forhindre markedsfragmentering.

For at nå disse mål indeholder dette forslag en afbalanceret og forholdsmæssigt afpasset horisontal lovgivningsmæssig tilgang til kunstig intelligens, som er begrænset til de mindstekrav, der er nødvendige for at håndtere de risici og problemer, der er forbundet med kunstig intelligens, uden unødigt at begrænse eller hindre den teknologiske udvikling eller på anden måde uforholdsmæssigt øge omkostningerne ved at omsætte AI-løsninger. Med forslaget fastlægges en robust og fleksibel retlig ramme. På den ene side er det omfattende og fremtidssikret med hensyn til de grundlæggende lovgivningsmæssige valg, herunder de principbaserede krav, som AI-systemer bør overholde. På den anden side indføres der et proportionalt reguleringssystem, der er baseret på en veldefineret risikobaseret reguleringstilgang, som ikke skaber unødvendige handelsrestriktioner, hvorved retlig indgriben er skræddersyet til de konkrete situationer, hvor der er en berettiget grund til bekymring, eller hvor en sådan bekymring med rimelighed kan forventes i den nærmeste fremtid. Samtidig indeholder de retlige rammer fleksible mekanismer, der gør det muligt at tilpasse dem dynamisk, efterhånden som teknologien udvikler sig og nye problemstillinger opstår.

Følgende en proportional risikobaseret tilgang fastsættes der med forslaget harmoniserede regler for udvikling, markedsføring og anvendelse af AI-systemer i Unionen. Der foreslås en enkelt fremtidssikret definition af kunstig intelligens. Visse særligt skadelige former for AI-praksis forbydes som værende i strid med Unionens værdier, mens der foreslås specifikke restriktioner og sikkerhedsforanstaltninger i forbindelse med visse anvendelser af systemer til biometrisk fjernidentifikation med henblik på retshåndhævelse. I forslaget fastsættes en robust metode til definition af "højrisiko-AI-systemer", som udgør en betydelig risiko for menneskers sundhed og sikkerhed eller grundlæggende rettigheder. Disse AI-systemer skal opfylde et sæt horisontale obligatoriske krav til pålidelig kunstig intelligens og der skal følges en procedure for overensstemmelsesvurdering, inden disse systemer kan bringes i omsætning på EU-markedet. Udbydere og brugere af disse systemer pålægges også gennemsikkelige, proportionale og klare forpligtelser til at garantere sikkerhed og overholdelse af eksisterende lovgivning, der beskytter de grundlæggende rettigheder, i hele AI-systemets livscyklus. For visse specifikke AI-systemer foreslås der kun minimale gennemsigtighedsforpligtelser, navnlig ved anvendelse af chatbots eller "deep fakes".

De foreslåede regler vil blive håndhævet gennem et forvaltningssystem på medlemsstatsplan, der bygger på allerede eksisterende strukturer, og en samarbejds mekanisme på EU-plan med oprettelsen af Det Europæiske Udvalg for Kunstig Intelligens. Der foreslås også yderligere foranstaltninger til støtte for innovation, navnlig gennem reguleringsmæssige sandkasser for kunstig intelligens og andre foranstaltninger til at mindske regelbyrden og støtte små og mellemstore virksomheder (SMV'er) og startup-virksomheder.

## **1.2. Sammenhæng med de gældende regler på samme område**

Forslagets horisontale karakter kræver fuld overensstemmelse med eksisterende EU-lovgivning, der finder anvendelse på sektorer, hvor der allerede anvendes eller sandsynligvis vil blive anvendt højrisiko-AI-systemer i den nærmeste fremtid.

Der sikres også overensstemmelse med EU's charter om grundlæggende rettigheder og den eksisterende afledte EU-lovgivning om databeskyttelse, forbrugerbeskyttelse, ikkeforskelsbehandling og ligestilling mellem kønnene. Forslaget berører ikke den generelle forordning om databeskyttelse (forordning (EU) 2016/679) og retshåndhævelsesdirektivet (direktiv (EU) 2016/680), men supplerer disse med et sæt harmoniserede regler for udformning, udvikling og anvendelse af visse højrisiko-AI-systemer og begrænsninger for visse anvendelser af systemer til biometrisk fjernidentifikation. Forslaget supplerer desuden den eksisterende EU-lovgivning om ikkeforskelsbehandling med specifikke krav, der har til formål at minimere risikoen for algoritmisk forskelsbehandling, navnlig i forbindelse med udformningen og kvaliteten af de datasæt, der anvendes til udvikling af AI-systemer, suppleret med krav om testning, risikostyring, dokumentation og menneskeligt tilsyn i hele AI-systemernes livscyklus. Forslaget berører ikke anvendelsen af EU-konkurrenceretten.

For så vidt angår højrisiko-AI-systemer, der indgår som sikkerhedskomponenter i produkter, vil dette forslag blive integreret i den eksisterende sektorspecifikke sikkerhedslovgivning for at sikre konsekvens, undgå overlap og minimere yderligere byrder. Navnlig for så vidt angår højrisiko-AI-systemer i forbindelse med produkter, der er omfattet af lovgivning under den nye lovgivningsmæssige ramme (f.eks. maskiner, medicinsk udstyr, legetøj), vil de krav til AI-systemer, der er fastsat i dette forslag, blive kontrolleret som led i de eksisterende procedurer for overensstemmelsesvurdering i henhold til den relevante lovgivning under den nye lovgivningsmæssige ramme. Hvad angår samspillet mellem kravene, er det meningen, at de sikkerhedsrisici, der er specifikke for AI-systemer, omfattes af kravene i dette forslag, mens lovgivning under den nye lovgivningsmæssige ramme har til formål at sikre det endelige produkts samlede sikkerhed og derfor kan indeholde specifikke krav vedrørende sikker integration af et AI-system i det endelige produkt. Forslaget til en maskinforordning, der vedtages samme dag som dette forslag, afspejler fuldt ud denne tilgang. For så vidt angår højrisiko-AI-systemer i forbindelse med produkter, der er omfattet af en relevant lovgivning efter den gamle metode (f.eks. luftfart og biler), finder dette forslag ikke direkte anvendelse. De forudgående væsentlige krav til højrisiko-AI-systemer, der er fastsat i dette forslag, skal der dog tages højde for når der vedtages relevant gennemførelseslovgivning eller delegeret lovgivning i henhold til disse retsakter.

For så vidt angår AI-systemer, der leveres eller anvendes af regulerede kreditinstitutter, bør de myndigheder, der er ansvarlige for tilsynet med EU-lovgivningen om finansielle tjenesteydelser, udpeges som kompetente myndigheder til at føre tilsyn med kravene i dette forslag for at sikre en sammenhængende håndhævelse af forpligtelserne i henhold til dette forslag og Unionens lovgivning om finansielle tjenesteydelser, hvor AI-systemer til en vis grad er regulerede implicit i forhold til kreditinstitutternes interne forvaltningssystem. For yderligere at styrke sammenhængen er proceduren for overensstemmelsesvurdering og nogle af udbydernes proceduremæssige forpligtelser i henhold til dette forslag integreret i

procedurerne i direktiv 2013/36/EU om adgang til at udøve virksomhed som kreditinstitut og om tilsyn<sup>14</sup>.

Dette forslag er også i overensstemmelse med den gældende EU-lovgivning om tjenesteydelser, herunder om formidlingstjenester, der er reguleret af direktiv 2000/31/EF<sup>15</sup> om elektronisk handel og Kommissionens nylige forslag til en retsakt om digitale tjenester<sup>16</sup>.

For så vidt angår AI-systemer, der er komponenter til store IT-systemer inden for området med frihed, sikkerhed og retfærdighed, der forvaltes af Den Europæiske Unions Agentur for den Operationelle Forvaltning af Store IT-Systemer (eu-LISA), finder forslaget ikke anvendelse på de AI-systemer, der er bragt i omsætning eller taget i brug, før der er gået et år fra datoen for denne forordnings anvendelse, medmindre erstatningen eller ændringen af disse retsakter medfører en væsentlig ændring af det pågældende AI-systems eller -systemers design eller tilsigtede formål.

### 1.3. Sammenhæng med Unionens politik på andre områder

Forslaget er en del af en bredere omfattende pakke af foranstaltninger, der tager fat på de problemer, som udviklingen og anvendelsen af kunstig intelligens medfører, som behandlet i hvidbogen om kunstig intelligens. Der sikres derfor overensstemmelse og komplementaritet med andre igangværende eller planlagte initiativer fra Kommissionens side, som også tager fat på disse problemer, herunder revisionen af den sektorspecifikke produktlovgivning (f.eks. maskindirektivet og direktivet om produktsikkerhed i almindelighed) og initiativer, der omhandler ansvarsspørgsmål i forbindelse med nye teknologier, herunder AI-systemer. Disse initiativer bygger videre på og supplerer dette forslag med henblik på at skabe juridisk klarhed og fremme udviklingen af et tillidsmiljø i forbindelse med kunstig intelligens i Europa.

Forslaget hænger også sammen med Kommissionens digitale strategi, idet det bidrager til at fremme teknologi, der tjener alle, som er en af de tre hovedsøjler til støtte for de politiske retningslinjer og målsætninger, der blev annonceret i meddelelsen om "Europas digitale fremtid i støbeskeen"<sup>17</sup>. Det fastlægger en sammenhængende, effektiv og proportional ramme for at sikre, at kunstig intelligens udvikles på måder, der respekterer borgernes rettigheder og fortjener deres tillid, gør Europa klar til den digitale tidsalder og omdanner de næste ti år til **det digitale årti**<sup>18</sup>.

Desuden er fremme af AI-drevet innovation tæt forbundet med **datastyringsforordningen**<sup>19</sup>, **direktivet om åbne data**<sup>20</sup> og andre initiativer under **EU's strategi for data**<sup>21</sup>, som vil

<sup>14</sup> Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF (EUT L 176 af 27.6.2013, s. 338).

<sup>15</sup> Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informations-samfundstjenester, navnlig elektronisk handel, i det indre marked ("Direktivet om elektronisk handel") (EFT L 178 af 17.7.2000, s. 1).

<sup>16</sup> Forslag til Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester (retsakt om digitale tjenester) og om ændring af direktiv 2000/31/EF (COM(2020) 825 final).

<sup>17</sup> Meddelelse fra Kommissionen: Europas digitale fremtid i støbeskeen, COM/2020/67 final.

<sup>18</sup> kompas: den.

<sup>19</sup> Forslag til Europa-Parlamentets og Rådets forordning om europæisk datastyring (forordning om datastyring), [COM\(2020\) 767](#).

<sup>20</sup> Europa-Parlamentets og Rådets direktiv (EU) 2019/1024 af 20. juni 2019 om åbne data og videreanvendelse af den offentlige sektors informationer PE/28/2019/REV/1 (EUT L 172 af 26.6.2019, s. 56).

<sup>21</sup> [Meddelelse om "En europæisk strategi for data", COM\(2020\) 66 final](#).

etablere pålidelige mekanismer og tjenester til videreanvendelse, udveksling og samling af data, som er afgørende for udviklingen af datadrevne AI-modeller af høj kvalitet.

Forslaget styrker også i væsentlig grad Unionens rolle med hensyn til at bidrage til udformningen af globale normer og standarder og fremme pålidelig kunstig intelligens, der er i overensstemmelse med Unionens værdier og interesser. Den giver Unionen et stærkt grundlag for yderligere dialog med sine eksterne partnere, herunder tredjelande, og i internationale fora om spørgsmål vedrørende kunstig intelligens.

## **2. RETSGRUNDLAG, NÆRHEDSPRINCIPPET OG PROPORCIONALITETSPRINCIPPET**

### **2.1. Retsgrundlag**

Retsgrundlaget for forslaget er først og fremmest artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF), som indeholder bestemmelser om vedtagelse af foranstaltninger, der skal sikre det indre markeds oprettelse og funktion.

Dette forslag udgør en central del af EU's strategi for et digitalt indre marked. Hovedformålet med dette forslag er at sikre et velfungerende indre marked ved at fastsætte harmoniserede regler, navnlig for udvikling, markedsføring på EU-markedet og brug af produkter og tjenester, der gør brug af AI-teknologier eller leveres som selvstændige AI-systemer. Nogle medlemsstater overvejer allerede nationale regler for at sikre, at kunstig intelligens er sikker, og at den udvikles og anvendes i overensstemmelse med forpligtelserne vedrørende grundlæggende rettigheder. Dette vil sandsynligvis medføre to hovedproblemer: i) en fragmentering af det indre marked på væsentlige punkter, navnlig vedrørende kravene til AI-produkter og -tjenester, deres markedsføring, deres anvendelse, ansvarsspørgsmål og de offentlige myndigheders tilsyn, og ii) den betydelige forringelse af retssikkerheden for både udbydere og brugere af AI-systemer med hensyn til, hvordan eksisterende og nye regler vil finde anvendelse på disse systemer inden for Unionen. I betragtning af den omfattende bevægelighed af varer og tjenesteydelser på tværs af grænserne kan disse to problemer bedst løses gennem harmonisering af lovgivningen på EU-plan.

Ved forslaget fastlægges der således vedrørende udformningen og udviklingen af visse AI-systemer, inden de bringes i omsætning, fælles obligatoriske krav, som vil blive gjort yderligere operationelle gennem harmoniserede tekniske standarder. Der tages også højde for situationer, efter at AI-systemer er blevet bragt i omsætning, ved at harmonisere den måde, hvorpå efterfølgende kontrol gennemføres.

I betragtning af at dette forslag indeholder visse specifikke regler om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger, navnlig begrænsninger i anvendelsen af AI-systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse, er det desuden hensigtsmæssigt at basere denne forordning på artikel 16 i TEUF for så vidt angår disse specifikke regler.

### **2.2. Nærhedsprincippet (for områder, der ikke er omfattet af enekompetence)**

Eftersom kunstig intelligens ofte afhænger af store og varierede datasæt, og kan være indlejret i ethvert produkt eller tjeneste, der cirkulerer frit på det indre marked, kan målene med dette forslag ikke opfyldes effektivt af medlemsstaterne alene. Desuden vil et kludetæppe af potentielt divergerende nationale regler forhindre produkter og tjenester i forbindelse med AI-systemer i at cirkulere gnidningsløst i hele EU og vil være ineffektivt med hensyn til at garantere sikkerheden og beskyttelsen af de grundlæggende rettigheder og Unionens værdier i de forskellige medlemsstater. Nationale tilgange til løsning af problemerne vil kun skabe



yderligere retsikkerhed og hindringer og vil forsinke markedsaecpten af kunstig intelligens.

Målene med dette forslag kan bedre nås på EU-plan for at undgå en yderligere opsplitning af det indre marked i potentielt modstridende nationale rammer, der forhindrer fri bevægelighed for varer og tjenesteydelser, der integrerer kunstig intelligens. En solid europæisk lovgivningsmæssig ramme for pålidelig kunstig intelligens vil også sikre lige vilkår og beskytte alle borgere samt styrke Europas konkurrenceevne og industrielle grundlag inden for kunstig intelligens. Kun fælles handling på EU-plan kan også beskytte Unionens digitale suverænitæt og udnytte dens redskaber og lovgivningsmæssige beføjelser til at forme globale regler og standarder.

### **2.3. Proportionalitetsprincippet**

Forslaget bygger på eksisterende retlige rammer og er rimeligt og nødvendigt for at nå målene, da det følger en risikobaseret tilgang og kun pålægger reguleringsmæssige byrder, når et AI-system sandsynligvis vil udgøre en stor risiko for grundlæggende rettigheder og sikkerhed. For andre AI-systemer, der ikke er højrisikosystemer, pålægges der kun meget begrænsede gennemsigtighedsforpligtelser, f.eks. med hensyn til markering af et AI-system, når det bruges til at interagere med mennesker. For højrisiko-AI-systemer er kravene om data af høj kvalitet, dokumentation og sporbarhed, gennemsigtighed, menneskeligt tilsyn, robusthed og modstandsdygtighed strengt nødvendige for at mindske de risici, som kunstig intelligens medfører for grundlæggende rettigheder og sikkerhed, og som ikke er omfattet af andre eksisterende retlige rammer. Harmoniserede standarder, vejledning og overholdelsesfremmende værktøjer vil hjælpe udbydere og brugere med at overholde de krav, der er fastsat i forslaget, og minimere deres omkostninger. Operatørernes omkostninger står i et rimeligt forhold til de opnåede mål og de økonomiske og omdømmemæssige fordele, som operatørerne kan forvente af dette forslag.

### **2.4. Valg af retsakt**

Valget af en forordning som juridisk instrument er begrundet i behovet for en ensartet anvendelse af de nye regler, såsom definitionen af kunstig intelligens, forbuddet mod visse former for skadelig AI-baseret praksis og klassificeringen af visse AI-systemer. Da en forordning finder direkte anvendelse i overensstemmelse med artikel 288 i TEUF vil det mindske retlig fragmentering og lette udviklingen af et indre marked for lovlige, sikre og pålidelige AI-systemer. Dette vil navnlig ske ved at indføre et harmoniseret sæt centrale krav med hensyn til højrisiko-AI-systemer og forpligtelser for udbydere og brugere af disse systemer, forbedre beskyttelsen af grundlæggende rettigheder og skabe retssikkerhed for både operatører og forbrugere.

Samtidig er forordningens bestemmelser ikke unødigt præskriptive og giver plads til medlemsstaternes indsats på flere niveauer for elementer, der ikke underminerer initiativets mål, navnlig den interne tilrettelæggelse af systemet til markedsovervågning og indførelsen af foranstaltninger til fremme af innovation.

## **3. RESULTATER AF EFTERFØLGENDE EVALUERINGER, HØRINGER AF INTERESSEREDE PARTER OG KONSEKVENSANALYSER**

### **3.1. Høringer af interesserede parter**

Dette forslag er resultatet af en omfattende høring af alle de vigtigste interesserede parter, hvor de generelle principper og minimumsstandarder for Kommissionens høring af interesserede parter blev anvendt.

Samtidig med offentliggørelsen af hvidbogen om kunstig intelligens blev der den 19. februar 2020 iværksat en offentlig onlinehøring, som løb indtil den 14. juni 2020. Formålet med denne høring var at indsamle synspunkter og udtalelser om hvidbogen. Den var henvendt til alle interesserede parter fra den offentlige og private sektor, herunder regeringer, lokale myndigheder, kommercielle og ikkekommercielle organisationer, arbejdsmarkedets parter, eksperter, akademikere og borgere. Efter at have analyseret alle de modtagne svar offentliggjorde Kommissionen et resumé af resultaterne og de individuelle svar på sit websted<sup>22</sup>.

I alt blev der modtaget 1215 bidrag, heraf 352 fra virksomheder eller erhvervsorganisationer/sammenslutninger, 406 fra enkeltpersoner (92 % enkeltpersoner fra EU), 152 på vegne af akademiske institutioner/forskningsinstitutioner og 73 fra offentlige myndigheder. Civilsamfundets stemme var repræsenteret af 160 respondenter (heriblandt 9 forbrugerorganisationer, 129 ikkestatslige organisationer og 22 fagforeninger), og 72 respondenter bidrog som "andre". Af de 352 repræsentanter for erhvervslivet og industrien var 222 repræsentanter for virksomheder, hvoraf 41,5 % var mikrovirksomheder og små og mellemstore virksomheder. Resten kom fra erhvervssammenslutninger. Samlet set kom 84 % af besvarelserne fra erhvervslivet og industrien i EU-27. Afhængigt af spørgsmålet brugte mellem 81 og 598 af respondenterne muligheden for at indsætte kommentarer i fri tekst. Der blev indsendt over 450 holdningsdokumenter via EUSurvey-webstedet, enten som supplement til spørgeskemabesvarelser (over 400) eller som selvstændige bidrag (over 50).

Der er generel enighed blandt interessenterne om, at der er behov for handling. Et stort flertal af interessenterne er enige i, at der er huller i lovgivningen, eller at der er behov for ny lovgivning. Flere interessenter advarer imidlertid Kommissionen om at undgå overlap, modstridende forpligtelser og overregulering. Der var mange bemærkninger, der understregede vigtigheden af en teknologineutral og proportional lovgivningsmæssig ramme.

Interessenterne efterlyste for det meste en snæver, klar og præcis definition af kunstig intelligens. Interessenterne fremhævede også, at det ud over præciseringen af begrebet kunstig intelligens er vigtigt at definere "risiko", "højrisiko", "lavrisiko", "biometrisk fjernidentifikation" og "skade".

De fleste respondenter går udtrykkeligt ind for den risikobaserede tilgang. Anvendelse af en risikobaseret ramme blev anset for at være en bedre løsning end en generel regulering af alle AI-systemer. Risiko- og trusselstyperne bør baseres på en sektorspecifik og individuel tilgang. Risikoen bør også beregnes under hensyntagen til indvirkningen på rettigheder og sikkerhed.

Reguleringsmæssige sandkasser kan være meget nyttige til fremme af kunstig intelligens og hilses velkommen af visse interessenter, navnlig erhvervssammenslutningerne.

Blandt dem, der formulerede deres mening om håndhævelsesmodellerne, gik mere end 50 %, navnlig fra erhvervssammenslutningerne, ind for en kombination af en forudgående egenrisikovurdering og en efterfølgende håndhævelse for højrisiko-AI-systemer.

### **3.2. Indhentning og brug af ekspertbistand**

Forslaget bygger på to års analyse og tæt inddragelse af interessenter, herunder akademikere, virksomheder, arbejdsmarkedets parter, ikkestatslige organisationer, medlemsstaterne og borgerne. Det forberedende arbejde startede i 2018 med oprettelsen af **Ekspertgruppen på Højt Niveau vedrørende Kunstig Intelligens**, som havde en inklusiv og bred sammensætning af 52 velkendte eksperter, der havde til opgave at rådgive Kommissionen om

---

<sup>22</sup> [Se høringens resultater her.](#)

gennemførelsen af Kommissionens strategi for kunstig intelligens. I april 2019 bakkede Kommissionen op om<sup>23</sup> de centrale krav i ekspertgruppens etiske retningslinjer for pålidelig kunstig intelligens<sup>24</sup>, som var blevet revideret for at tage hensyn til mere end 500 indlæg fra interessenter. Som det fremgår af den lange række af etiske kodekser og principper, der er udviklet af mange private og offentlige organisationer i og uden for Europa, afspejler de centrale krav den brede og fælles tilgang, at udvikling og anvendelse af kunstig intelligens bør styres af visse essentielle værdiorienterede principper. Ved hjælp af vurderingslisten for pålidelig kunstig intelligens<sup>25</sup> blev disse krav gjort operationelle i en pilotproces med over 350 organisationer.

Desuden blev **Den Europæiske Alliance vedrørende Kunstig Intelligens**<sup>26</sup> dannet som en platform, hvor ca. 4000 interessenter drøftede de teknologiske og samfundsmæssige konsekvenser af kunstig intelligens, hvilket kulminerede i en årlig AI-forsamling.

Med **Hvidbogen om kunstig intelligens** blev der bygget videre på denne inklusive tilgang, hvilket afstedkom feedback fra mere end 1250 interessenter, herunder over 450 yderligere holdningsdokumenter. Som følge heraf offentliggjorde Kommissionen en indledende konsekvensanalyse, som igen affødte mere end 130 kommentarer<sup>27</sup>. Der blev også afholdt **yderligere workshops og arrangementer** for interessenter, og resultaterne herfra understøttede konsekvensanalysen og de politiske valg, der er truffet i forbindelse med dette forslag<sup>28</sup>. Desuden indgik en **ekstern undersøgelse** i konsekvensanalysen.

### 3.3. Konsekvensanalyse

I overensstemmelse med sin politik for bedre regulering har Kommissionen foretaget en konsekvensanalyse af dette forslag, som blev behandlet af Kommissionens Udvalg for Forskriftskontrol. Der blev afholdt et møde med Udvalget for Forskriftskontrol den 16. december 2020, som blev efterfulgt af en negativ udtalelse. Efter en omfattende revision af konsekvensanalysen for at imødekomme henstillingerne og en fornyet forelæggelse af konsekvensanalysen afgav Udvalget for Forskriftskontrol en positiv udtalelse den 21. marts 2021. Udtalelserne fra Udvalget for Forskriftskontrol, henstillingerne og en redegørelse for, hvordan der er taget hensyn til dem, findes i bilag 1 til konsekvensanalysen.

Kommissionen har undersøgt forskellige politiske løsningsmodeller for at nå det overordnede mål med forslaget, som er at **sikre et velfungerende indre marked** ved at skabe betingelserne for udvikling og anvendelse af pålidelig kunstig intelligens i Unionen.

Fire politiske løsningsmodeller med forskellige grader af regulerende indgreb blev vurderet:

- **Model 1:** en EU-retsakt om indførelse af en frivillig mærkningsordning.
- **Model 2:** en sektorspecifik ad hoc-tilgang.
- **Model 3:** en horisontal EU-retsakt baseret på en proportional risikobaseret tilgang.

<sup>23</sup> Europa-Kommissionen, [Opbygning af tillid til menneskecentreret kunstig intelligens](#), COM(2019) 168.

<sup>24</sup> Ekspertgruppen på Højt Niveau vedrørende Kunstig Intelligens — [Ethics Guidelines for Trustworthy AI](#), 2019.

<sup>25</sup> Ekspertgruppen på Højt Niveau vedrørende Kunstig Intelligens — [Assessment List for Trustworthy Artificial Intelligence \(ALTAI\) for self-assessment](#), 2020.

<sup>26</sup> Den Europæiske Alliance vedrørende Kunstig Intelligens er et multiinteressentforum, der blev lanceret i juni 2018 — <https://ec.europa.eu/digital-single-market/en/european-ai-alliance>.

<sup>27</sup> Europa-Kommissionen — [Indledende konsekvensanalyse med henblik på forslag til Europa-Parlamentets og Rådets retsakt om fastlæggelse af krav til kunstig intelligens](#).

<sup>28</sup> Nærmere oplysninger om alle gennemførte høringer findes i bilag 2 til konsekvensanalysen.

- **Model 3+:** en horisontal EU-retsakt baseret på en proportional risikobaseret tilgang + adfærdskodekser for AI-systemer, der ikke er højrisikosystemer.
- **Model 4:** en horisontal EU-retsakt, der fastsætter obligatoriske krav til alle AI-systemer, uanset hvilken risiko de udgør.

I henhold til Kommissionens fastlagte metode blev hver politiske løsningsmodel evalueret i forhold til de økonomiske og samfundsmæssige virkninger med særligt fokus på indvirkningen på de grundlæggende rettigheder. Den foretrukne løsningsmodel er model 3+, en lovgivningsmæssige ramme, der kun gælder for højrisiko-AI-systemer, med mulighed for, at alle udbydere af AI-systemer, der ikke er højrisikosystemer, kan følge en adfærdskodeks. Kravene vil vedrøre data, dokumentation og sporbarhed, tilvejebringelse af oplysninger, gennemsigtighed, menneskeligt tilsyn og robusthed samt nøjagtighed og vil være obligatoriske for højrisiko-AI-systemer. Virksomheder, der indfører adfærdskodekser for andre AI-systemer, vil gøre dette frivilligt.

Den foretrukne model blev anset for velegnet til at opfylde målsætningerne i dette forslag på den mest effektive måde. Ved at fastlægge begrænsede, men effektive krav til udviklere og brugere af kunstig intelligens mindsker den foretrukne løsningsmodel risikoen for krænkelse af grundlæggende rettigheder og menneskers sikkerhed og fremmer effektivt tilsyn og effektiv håndhævelse ved kun at målrette kravene mod systemer, hvor der er stor risiko for, at sådanne krænkelse kan forekomme. Som følge heraf holder denne model efterlevelsesomkostningerne på et minimum, hvorved man undgår unødvendige forsinkelser i udbredelsen på grund af højere priser og efterlevelsesomkostninger. For at afhjælpe eventuelle ulemper for SMV'er omfatter denne løsningsmodel flere bestemmelser til støtte for deres efterlevelse og reduktion af deres omkostninger, herunder oprettelse af reguleringsmæssige sandkasser og en forpligtelse til at tage hensyn til SMV'ers interesser, når der fastsættes gebyrer i forbindelse med overensstemmelsesvurdering.

Den foretrukne løsningsmodel vil øge borgernes tillid til kunstig intelligens, øge retssikkerheden for virksomhederne, og medlemsstaterne vil ikke have grund til at træffe ensidige foranstaltninger, der kan fragmentere det indre marked. Det indre marked for kunstig intelligens vil sandsynligvis blomstre som følge af øget efterspørgsel medført af øget tillid, flere tilgængelige tilbud på grund af retssikkerheden og fraværet af hindringer for AI-systemers grænseoverskridende bevægelighed. Den Europæiske Union vil fortsætte med at udvikle et hurtigt voksende AI-økosystem, der omfatter innovative tjenester og produkter med integreret AI-teknologi eller selvstændige AI-systemer, hvilket resulterer i øget digital autonomi.

Virksomheder eller offentlige myndigheder, der er udviklere eller brugere af AI-anvendelser, der udgør en høj risiko for borgernes sikkerhed eller grundlæggende rettigheder, vil skulle opfylde specifikke krav og forpligtelser. Opfyldelsen af disse krav vil i forbindelse med levering af et gennemsnitligt højrisiko-AI-system til ca. 170 000 EUR medføre omkostninger på ca. 6 000-7 000 EUR frem til 2025. For brugerne af AI vil der også være årlige omkostninger forbundet med den tid, der bruges på at sikre menneskeligt tilsyn, i de tilfælde, hvor dette er hensigtsmæssigt. Disse anslås til ca. 5 000-8 000 EUR om året. Kontrolomkostningerne kan beløbe sig til yderligere 3 000-7 500 EUR for leverandører af højrisiko-AI. Virksomheder eller offentlige myndigheder, der er udviklere eller brugere af AI-anvendelser, der ikke er klassificeret som højrisiko, vil kun skulle opfylde minimale oplysningskrav. De kunne imidlertid vælge i sammenslutning med andre at vedtage en adfærdskodeks for at opfylde passende krav og for at sikre, at deres AI-systemer er pålidelige. I et sådant tilfælde ville omkostningerne højst være som for højrisiko-AI-systemer, men sandsynligvis lavere.

Virkningerne af de politiske løsningsmodeller for forskellige kategorier af interessenter (erhvervsdrivende/virksomheder, overensstemmelsesvurderingsorganer, standardiseringsorganer og andre offentlige organer, enkeltpersoner/borgere, forskere) er nærmere forklaret i bilag 3 til konsekvensanalysen til støtte for dette forslag.

### **3.4. Målrettet regulering og forenkling**

Dette forslag fastsætter forpligtelser, som vil gælde for udbydere og brugere af højrisiko-AI-systemer. For udbydere, der udvikler og bringer sådanne systemer i omsætning på EU-markedet, vil det skabe retssikkerhed og sikre, at der ikke opstår hindringer for grænseoverskridende levering af AI-relaterede tjenester og produkter. For virksomheder, der anvender kunstig intelligens, vil det fremme tilliden blandt deres kunder. For de nationale offentlige forvaltninger vil det fremme offentlighedens tillid til brugen af kunstig intelligens og styrke håndhævelsesmekanismerne (ved at indføre en europæisk koordineringsmekanisme, tilvejebringe passende kapacitet og lette revisionen af AI-systemerne med nye krav til dokumentation, sporbarhed og gennemsigtighed). Rammen omfatter desuden specifikke foranstaltninger til støtte for innovation, herunder reguleringsmæssige sandkasser og specifikke foranstaltninger, der skal hjælpe mindre brugere og udbydere af højrisiko-AI-systemer med at overholde de nye regler.

Forslaget sigter også specifikt mod at styrke Europas konkurrenceevne og industrielle grundlag inden for kunstig intelligens. Der sikres fuld overensstemmelse med eksisterende sektorspecifik EU-lovgivning, som AI-systemer omfattes af (f.eks. om produkter og tjenesteydelser), hvilket skaber yderligere klarhed og forenkler håndhævelsen af de nye regler.

### **3.5. Grundlæggende rettigheder**

Brugen af kunstig intelligens med dens særlige karakteristika (f.eks. uigennemsigthed, kompleksitet, afhængighed af data, selvstændig adfærd) kan have en negativ indvirkning på en række grundlæggende rettigheder, der er nedfældet i EU's charter om grundlæggende rettigheder ("chartret"). Dette forslag har til formål at sikre et højt beskyttelsesniveau for disse grundlæggende rettigheder og tager sigte på at håndtere forskellige risikokilder gennem en klart defineret risikobaseret tilgang. Med et sæt krav til pålidelig kunstig intelligens og forholdsmæssigt afpassede forpligtelser for alle værdikædens deltagere vil forslaget styrke og fremme beskyttelsen af de rettigheder, der er beskyttet af chartret, navnlig retten til menneskelig værdighed (artikel 1), respekt for privatliv og beskyttelse af personoplysninger (artikel 7 og 8), ikke-forskelsbehandling (artikel 21) og ligestilling mellem kvinder og mænd (artikel 23). Det har til formål at forhindre en afdæmpende virkning på ytringsfriheden (artikel 11) og forsamlingsfriheden (artikel 12), at sikre adgangen til effektive retsmidler og til en upartisk domstol, retten til et forsvar og uskyldsformodningen (artikel 47 og 48) samt sikre det generelle princip om god forvaltningsskik. Alt efter hvad der er relevant på visse områder, vil forslaget have en positiv indvirkning på rettighederne for en række særlige grupper, såsom arbejdstagernes ret til retfærdige og rimelige arbejdsforhold (artikel 31), et højt forbrugerbeskyttelsesniveau (artikel 28), børns rettigheder (artikel 24) og integration af personer med handicap (artikel 26). Retten til et højt niveau af miljøbeskyttelse og forbedring af miljøet (artikel 37) er også relevant, herunder i forbindelse med menneskers sundhed og sikkerhed. Forpligtelserne til forudgående testning, risikostyring og menneskeligt tilsyn vil også lette overholdelsen af andre grundlæggende rettigheder ved at minimere risikoen for fejlagtige eller partiske AI-støttede beslutninger på kritiske områder såsom uddannelse, beskæftigelse, vigtige tjenester, retshåndhævelse og retsvæsen. Skulle der alligevel forekomme overtrædelser af de grundlæggende rettigheder, sikres de berørte personer mulighed for effektiv klageadgang gennem AI-systemernes gennemsigtighed og sporbarhed, kombineret med en stærk efterfølgende kontrol.

Dette forslag medfører visse begrænsninger i friheden til at oprette og drive egen virksomhed (artikel 16) og friheden for kunst og videnskab (artikel 13) for at sikre overholdelse af tvingende almene hensyn såsom sundhed, sikkerhed, forbrugerbeskyttelse og beskyttelse af andre grundlæggende rettigheder ("ansvarlig innovation"), når der udvikles og anvendes AI-teknologi med høj risiko. Disse begrænsninger er forholdsmæssigt afpassede og er begrænsede til det minimum, der er nødvendigt for at forebygge og afbøde alvorlige sikkerhedsrisici og sandsynlige overtrædelser af grundlæggende rettigheder.

De øgede gennemsigtighedsforpligtelser vil heller ikke i uforholdsmæssig høj grad påvirke retten til beskyttelse af intellektuel ejendomsret (artikel 17, stk. 2), da de begrænses til det minimum, der er nødvendigt for, at enkeltpersoner kan udøve deres ret til effektive retsmidler og den nødvendige gennemsigtighed over for tilsyns- og håndhævelsesmyndighederne i overensstemmelse med deres mandater. Enhver videregivelse af oplysninger vil ske i overensstemmelse med relevant lovgivning på området, herunder direktiv 2016/943 om beskyttelse af fortrolig knowhow og fortrolige forretningsoplysninger (forretningshemmeligheder) mod ulovlig erhvervelse, brug og videregivelse. Når offentlige myndigheder og bemyndigede organer skal have adgang til fortrolige oplysninger eller kildekoder for at kunne undersøge, om væsentlige forpligtelser er opfyldt, er de underlagt bindende tavshedspligt.

#### **4. VIRKNINGER FOR BUDGETTET**

Medlemsstaterne udpeger de tilsynsmyndigheder, der skal have ansvaret for at gennemføre de lovgivningsmæssige krav. Tilsynsfunktionen kunne bygge på eksisterende ordninger, f.eks. angående overensstemmelsesvurderingsorganer eller markedsovervågning, men ville kræve tilstrækkelig teknologisk ekspertise og menneskelige og finansielle ressourcer. Afhængigt af den eksisterende struktur i hver medlemsstat kan dette beløbe sig til 1-25 fuldtidsækvivalenter pr. medlemsstat.

En detaljeret oversigt over de omkostninger, der er forbundet hermed, findes i "finansieringsoversigten" til dette forslag.

#### **5. ANDRE FORHOLD**

##### **5.1. Planer for gennemførelsen og foranstaltninger til overvågning, evaluering og rapportering**

Det er afgørende at sørge for en robust overvågnings- og evalueringsmekanisme for at sikre, at forslaget vil være effektivt med hensyn til at nå de specifikke mål. Kommissionen er ansvarlig for at overvåge forslagens virkninger. Den opretter et system til registrering af selvstændige højrisiko-AI-anvendelser i en offentlig EU-dækkende database. Denne registrering vil også gøre det muligt for kompetente myndigheder, brugere og andre interesserede personer at kontrollere, om et givet højrisiko-AI-system overholder forslagens krav, og at føre øget tilsyn med de AI-systemer, der udgør en stor risiko for de grundlæggende rettigheder. Til brug for databasen vil udbydere af kunstig intelligens være forpligtet til at give meningsfulde oplysninger om deres systemer og om den overensstemmelsesvurdering, der er foretaget af disse systemer.

Udbydere af kunstig intelligens vil desuden være forpligtet til at underrette de nationale kompetente myndigheder om alvorlige hændelser eller fejl, der udgør en overtrædelse af forpligtelserne vedrørende grundlæggende rettigheder, så snart de får kendskab til dem, samt om alle tilbagekaldelser eller tilbagetrækninger af AI-systemer fra markedet. De nationale kompetente myndigheder undersøger derefter hændelserne/fejlene, indsamler alle nødvendige

oplysninger og sender dem regelmæssigt til Kommissionen med fyldestgørende metadata. Kommissionen vil supplere oplysningerne om hændelserne med en omfattende analyse af det samlede marked for kunstig intelligens.

Kommissionen vil offentliggøre en rapport med evaluering og gennemgang af den foreslåede ramme for kunstig intelligens fem år efter den dato, hvor den finder anvendelse.

## **5.2. Nærmere redegørelse for de enkelte bestemmelser i forslaget**

### *5.2.1. ANVENDELSESOMRÅDE OG DEFINITIONER (AFSNIT I)*

I **afsnit I** defineres forordningens genstand og anvendelsesområdet for de nye regler, der omfatter markedsføring, ibrugtagning og anvendelse af AI-systemer. Desuden fastsættes de definitioner, der anvendes i instrumentet. I den retlige ramme tilstræbes der en så teknologineutral og fremtidssikret definition af et AI-system som muligt under hensyntagen til den hurtige teknologiske udvikling og markedsudvikling i forbindelse med kunstig intelligens. For at skabe den nødvendige retssikkerhed suppleres afsnit I af bilag I, som indeholder en detaljeret liste over tilgange og teknikker til udvikling af kunstig intelligens, som Kommissionen løbende skal tilpasse den teknologiske udvikling. Centrale deltagere i hele værdikæden for kunstig intelligens er også klart defineret, f.eks. udbydere og brugere af AI-systemer, der dækker både offentlige og private operatører med henblik på at sikre lige vilkår.

### *5.2.2. FORBUDT PRAKSIS MED HENSYN TIL KUNSTIG INTELLIGENS (AFSNIT II)*

**Afsnit II** indeholder en liste over forbudt kunstig intelligens. I forordningen følges en risikobaseret tilgang, hvor der skelnes mellem anvendelser af kunstig intelligens, som skaber i) en uacceptabel risiko, ii) en høj risiko og iii) lav eller minimal risiko. Listen over forbudte praksisser i afsnit II omfatter alle de AI-systemer, hvis anvendelse anses for at være i strid med Unionens værdier, f.eks. ved at krænke grundlæggende rettigheder. Forbuddet omfatter praksisser, der har et betydeligt potentiale til at manipulere en persons underbevidsthed ved hjælp af subliminale teknikker eller udnytte sårbarheder hos specifikke sårbare grupper såsom børn eller personer med handicap for væsentligt at forvride deres adfærd på en måde, der sandsynligvis vil forvolde dem eller en anden person psykisk eller fysisk skade. Anden manipulerende eller udnyttende praksis, som påvirker voksne, og som kan finde sted med bistand af AI-systemer, kan være omfattet af den eksisterende lovgivning om databeskyttelse, forbrugerbeskyttelse og digitale tjenester, som sikrer, at fysiske personer er behørigt informerede og frit kan vælge ikke at blive genstand for profilering eller anden praksis, der kan påvirke deres adfærd. Forslaget omfatter desuden et forbud mod offentlige myndigheders generelle brug af sociale pointsystemer baseret på kunstig intelligens. Endelig er det også forbudt at anvende systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse, med visse begrænsede undtagelser.

### *5.2.3. HØJRIKIKO-AI-SYSTEMER (AFSNIT III)*

**Afsnit III** indeholder specifikke regler for AI-systemer, der medfører høj risiko for fysiske personers sundhed og sikkerhed eller grundlæggende rettigheder. I overensstemmelse med en risikobaseret tilgang tillades disse højrisiko-AI-systemer på det europæiske marked, forudsat at visse obligatoriske krav opfyldes, og at der foretages en forudgående overensstemmelsesvurdering. Klassificeringen af et AI-system som værende et højrisikosystem baseres på dets tilsigtede formål, hvilket er i overensstemmelse med den eksisterende produktsikkerhedslovgivning. Klassificeringen som højrisiko afhænger derfor ikke kun af den funktion, AI-systemet udfører, men også af det specifikke formål med og de særlige modaliteter i anvendelsen af systemet.

I afsnit III, kapitel 1, fastsættes klassificeringsreglerne, og der identificeres to hovedkategorier af højrisiko-AI-systemer:

- AI-systemer, der er beregnet til at blive anvendt som sikkerhedskomponenter i produkter, der er underlagt en forudgående overensstemmelsesvurdering fra tredjepart
- andre selvstændige AI-systemer, der hovedsagelig har betydning for de grundlæggende rettigheder, og som eksplicit er opført i bilag III.

Listen over højrisiko-AI-systemer i bilag III indeholder et begrænset antal AI-systemer med risici, der allerede har realiseret sig eller sandsynligvis vil realisere sig i nær fremtid. For at sikre, at forordningen kan tilpasses fremtidige anvendelser af kunstig intelligens, kan Kommissionen udvide listen over højrisiko-AI-systemer inden for visse foruddefinerede områder, ved at anvende et sæt kriterier og risikovurderingsmetoder.

Kapitel 2 fastsætter de retlige krav til højrisiko-AI-systemer for så vidt angår data og dataforvaltning, dokumentation og registrering, gennemsigtighed og formidling af oplysninger til brugerne, menneskeligt tilsyn, robusthed, nøjagtighed og sikkerhed. De foreslåede minimumskrav er allerede state-of-the-art for mange samvittighedsfulde operatører, og er resultatet af to års forberedende arbejde, der er afledt af de etiske retningslinjer fra Ekspertgruppen på Højt Niveau vedrørende Kunstig Intelligens<sup>29</sup>, og som er blevet afprøvet i praksis af mere end 350 organisationer<sup>30</sup>. De er også i vid udstrækning i overensstemmelse med andre internationale anbefalinger og principper, hvilket sikrer, at den foreslåede ramme for kunstig intelligens er forenelig med de rammer, der er vedtaget af EU's internationale handelspartnere. Med henblik på at opnå overensstemmelse med disse krav kan de nøjagtige tekniske løsninger udvikles af AI-systemets udbyder i lyset af generel teknisk eller videnskabelig viden, eller ved hjælp af standarder eller andre tekniske specifikationer. Denne fleksibilitet er særlig vigtig, fordi den giver udbyderne af AI-systemer mulighed for at vælge, hvordan de vil opfylde kravene, under hensyntagen til de seneste teknologiske og videnskabelige fremskridt på området.

I kapitel 3 fastsættes et klart sæt horisontale forpligtelser for udbydere af højrisiko-AI-systemer. Der pålægges også rimelige forpligtelser for brugere og andre deltagere i hele AI-værdikæden (f.eks. importører, distributører, bemyndigede repræsentanter).

I kapitel 4 fastlægges rammerne for bemyndigede organers inddragelse som uafhængige tredjeparter i overensstemmelsesvurderingsprocedurer, mens kapitel 5 indeholder en detaljeret beskrivelse af de overensstemmelsesvurderingsprocedurer, der skal følges for hver type højrisiko-AI-system. Brugen af overensstemmelsesvurderinger har til formål at minimere byrden for både erhvervsdrivende og bemyndigede organer, hvis kapacitet gradvist skal øges med tiden. AI-systemer, der er beregnet til at blive anvendt som sikkerhedskomponenter i produkter, der er reguleret inden for den nye lovgivningsmæssige ramme (f.eks. maskiner, legetøj, medicinsk udstyr osv.), vil være underlagt de samme forudgående og efterfølgende overholdelses- og håndhævelsesmekanismer som de produkter, de er en del af. Forskellen er, at de forudgående og efterfølgende mekanismer ikke blot vil sikre overensstemmelse med de krav, der er fastsat i den sektorspecifikke lovgivning, men også med kravene i denne forordning.

For så vidt angår selvstændige højrisiko-AI-systemer, som der henvises til i bilag III, vil der blive etableret et nyt overholdelses- og håndhævelsessystem. Dette følger modellen for

<sup>29</sup> Ekspertgruppen på Højt Niveau vedrørende Kunstig Intelligens — [Ethics Guidelines for Trustworthy AI](#), 2019.

<sup>30</sup> De blev også godkendt af Kommissionen i dens meddelelse fra 2019 om menneskecentreret tilgang til kunstig intelligens.



lovgivning under den nye lovgivningsmæssige ramme, hvor intern kontrol gennemføres af udbyderne, med undtagelse af systemer til biometrisk fjernidentifikation, som vil blive genstand for overensstemmelsesvurderinger foretaget af tredjepart. En omfattende forudgående overensstemmelsesvurdering gennem intern kontrol kombineret med en stærk efterfølgende håndhævelse kan være en effektiv og rimelig løsning for disse systemer i betragtning af, at den lovgivningsmæssige indgriben er i en tidlig fase, samt de forhold, at AI-sektoren er meget innovativ, og at ekspertisen inden for revision først nu er ved at blive opbygget. En vurdering i form af intern kontrol af selvstændige højrisiko-AI-systemer vil kræve en fuldstændig, effektiv og behørigt dokumenteret forudgående opfyldelse af alle forordningens krav, samt korrekt brug af robuste kvalitets- og risikostyringssystemer og overvågning efter omsætning. Efter at udbyderen har foretaget den relevante overensstemmelsesvurdering, bør udbyderen registrere disse selvstændige højrisiko-AI-systemer i en EU-database, som vil blive forvaltet af Kommissionen for at øge gennemsigtigheden og offentlighedens tilsyn og styrke de kompetente myndigheders efterfølgende kontrol. Derimod vil AI-systemer, der er sikkerhedskomponenter til produkter, af hensyn til overensstemmelsen med den eksisterende produktsikkerhedslovgivning, underkastes tredjeparters overensstemmelsesvurderingsprocedurer, der allerede er indført i henhold til den relevante sektorspecifikke produktsikkerhedslovgivning. Der vil være behov for nye forudgående overensstemmelsesvurderinger i tilfælde af væsentlige ændringer af AI-systemerne (og navnlig ændringer, der går ud over, hvad udbyderen på forhånd har fastsat i sin tekniske dokumentation, og som kontrolleres på tidspunktet for den forudgående overensstemmelsesvurdering).

#### *5.2.4. GENNEMSIGTIGHEDSFORPLIGTELSE FOR VISSE AI-SYSTEMER (AFSNIT IV)*

**Afsnit IV** vedrører visse AI-systemer for at tage højde for de særlige risici for manipulation, som de udgør. Der vil gælde gennemsigtighedsforpligtelser for systemer, der i) interagerer med mennesker, ii) anvendes til at opdage følelser eller fastslå tilknytning til (sociale) kategorier baseret på biometriske data eller iii) generere eller manipulere indhold ("deep fakes"). Når personer interagerer med et AI-system eller hvis deres følelser eller karakteristika registreres automatisk, skal de informeres om dette forhold. Hvis et AI-system anvendes til at generere eller manipulere billed-, lyd- eller videoindhold, der i væsentlig grad ligner autentisk indhold, bør der være en forpligtelse til at oplyse, at indholdet er genereret automatisk, med forbehold af undtagelser til legitime formål (retshåndhævelse, ytringsfrihed). Dette gør det muligt for folk at træffe informerede valg eller træde tilbage fra en given situation.

#### *5.2.5. FORANSTALTNINGER TIL STØTTE FOR INNOVATION (AFSNIT V)*

Med afsnit V bidrages til målet om at skabe en retlig ramme, der er innovationsvenlig, fremtidssikret og modstandsdygtig over for forstyrrelser. Med henblik herpå tilskyndes de nationale kompetente myndigheder til at oprette reguleringsmæssige sandkasser og der opstilles en grundlæggende ramme for forvaltning, tilsyn og ansvar. De reguleringsmæssige sandkasser for kunstig intelligens etablerer et kontrolleret miljø til afprøvning af innovative teknologier i et begrænset tidsrum på grundlag af en testplan, der er aftalt med de kompetente myndigheder. Afsnit V omhandler også foranstaltninger til at mindske den reguleringsmæssige byrde for SMV'er og startup-virksomheder.

#### *5.2.6. FORVALTNING OG GENNEMFØRELSE (AFSNIT VI, VII OG VII)*

I afsnit VI indføres forvaltningssystemerne på EU-plan og nationalt plan. På EU-plan oprettes der med forslaget Det Europæiske Udvalg for Kunstig Intelligens ("udvalget") bestående af repræsentanter for medlemsstaterne og Kommissionen. Udvalget vil fremme en gnidningsløs, effektiv og harmoniseret gennemførelse af denne forordning ved at bidrage til et effektivt samarbejde mellem de nationale tilsynsmyndigheder og Kommissionen og yde rådgivning og

ekspertise til Kommissionen. Den vil også indsamle og udveksle bedste praksis mellem medlemsstaterne.

På nationalt plan skal medlemsstaterne udpege en eller flere nationale kompetente myndigheder, herunder den nationale tilsynsmyndighed, til at føre tilsyn med anvendelsen og gennemførelsen af forordningen. Den Europæiske Tilsynsførende for Databeskyttelse er den kompetente myndighed, der fører tilsyn med Unionens institutioner, agenturer og organer, når de er omfattet af denne forordnings anvendelsesområde.

**Afsnit VII** har til formål at lette Kommissionens og de nationale myndigheders overvågningsarbejde gennem oprettelse af en EU-dækkende database for selvstændige højrisiko-AI-systemer, som hovedsagelig vil have konsekvenser for de grundlæggende rettigheder. Databasen forvaltes af Kommissionen og forsynes med data fra udbyderne af AI-systemerne, som skal registrere deres systemer, før de bringes i omsætning eller på anden måde tages i brug.

I **afsnit VIII** fastsættes overvågnings- og rapporteringsforpligtelser for udbydere af AI-systemer med hensyn til overvågning efter omsætning og rapportering og undersøgelse af AI-relaterede hændelser og funktionsfejl. Markedsovervågningsmyndighederne kontrollerer også markedet og undersøger om forpligtelserne og kravene for alle højrisiko-AI-systemer, der allerede er bragt i omsætning, bliver overholdt. Markedsovervågningsmyndighederne vil have alle beføjelser i henhold til forordning (EU) 2019/1020 om markedsovervågning. Efterfølgende håndhævelse bør sikre, at de offentlige myndigheder, når AI-systemet er bragt i omsætning, har beføjelser og ressourcer til at gribe ind i tilfælde af, at AI-systemet skaber uventede risici, der berettiger en hurtig indsats. De vil også overvåge, at operatørerne overholder deres relevante forpligtelser i henhold til forordningen. Forslaget indeholder ikke bestemmelser om automatisk oprettelse af yderligere organer eller myndigheder på medlemsstatsniveau. Medlemsstaterne kan derfor udpege (og trække på ekspertisen hos) eksisterende sektormyndigheder, som også vil få overdraget beføjelser til at overvåge og håndhæve forordningens bestemmelser.

Alt dette berører ikke medlemsstaternes eksisterende systemer og tildelinger af beføjelser til efterfølgende håndhævelse af forpligtelser vedrørende grundlæggende rettigheder. Når det er nødvendigt for deres mandat, vil de eksisterende tilsyns- og håndhævelsesmyndigheder også have beføjelse til at anmode om og få adgang til al dokumentation, der opbevares i henhold til denne forordning, og om nødvendigt anmode markedsovervågningsmyndighederne om at tilrettelægge tekniske test af et højrisiko-AI-system.

#### 5.2.7. *ADFÆRDSKODEKSER (AFSNIT IX)*

Med afsnit IX skabes en ramme for udarbejdelse af adfærdskodekser, der har til formål at tilskynde udbydere af AI-systemer, der ikke er højrisikosystemer, til frivilligt at anvende de krav, der er obligatoriske for højrisiko-AI-systemer (som fastsat i afsnit III). Udbyderne af AI-systemer, der ikke er højrisikosystemer, kan selv udarbejde og gennemføre adfærdskodekserne. Disse kodekser kan også på frivillig basis omfatte yderligere forpligtelser vedrørende f.eks. miljømæssig bæredygtighed, tilgængelighed for personer med handicap, interessenters deltagelse i udformningen og udviklingen af AI-systemer og mangfoldighed i udviklingsteamene.

#### 5.2.8. *AFSLUTTENDE BESTEMMELSER (AFSNIT X, XI OG XII)*

I **afsnit X** understreges alle parter forpligtelse til at respektere fortroligheden af oplysninger og data, og der fastsættes regler for udveksling af oplysninger, der er indhentet i forbindelse med gennemførelsen af forordningen. Afsnit X omfatter også foranstaltninger til at sikre en effektiv gennemførelse af forordningen gennem sanktioner for overtrædelse af

bestemmelserne, der er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning.

**Afsnit XI** indeholder regler for udøvelsen af delegerede beføjelser og gennemførelsesbeføjelser. Med forslaget tillægges Kommissionen beføjelser til om nødvendigt at vedtage gennemførelsesretsakter for at sikre ensartet anvendelse af forordningen eller delegerede retsakter med henblik på at ajourføre eller supplere listerne i bilag I-VII.

**Afsnit XII** omhandler Kommissionens forpligtelse til regelmæssigt at vurdere behovet for en ajourføring af bilag III og til at udarbejde regelmæssige rapporter om evalueringen og revisionen af forordningen. Der fastsættes også afsluttende bestemmelser, herunder en differentieret overgangsperiode for forordningens anvendelsesdato for at lette en gnidningsløs gennemførelse for alle berørte parter.

Forslag til

**EUROPA-PARLAMENTETS OG RÅDETS FORORDNING**

**OM HARMONISEREDE REGLER FOR KUNSTIG INTELLIGENS (RETSAKTEN OM KUNSTIG INTELLIGENS) OG OM ÆNDRING AF VISSE AF UNIONENS LOVGIVNINGSMÆSSIGE RETSAKTER**

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —  
 under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 16 og 114,  
 under henvisning til forslag fra Europa-Kommissionen,  
 efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,  
 under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg<sup>31</sup>,  
 under henvisning til udtalelse fra Regionsudvalget<sup>32</sup>,  
 efter den almindelige lovgivningsprocedure, og  
 ud fra følgende betragtninger:

- (1) Formålet med denne forordning er at forbedre det indre markeds funktion ved at fastlægge ensartede retlige rammer, navnlig for udvikling, markedsføring og anvendelse af kunstig intelligens i overensstemmelse med Unionens værdier. Med denne forordning forfølges en række tvingende almene hensyn, såsom et højt beskyttelsesniveau for sundhed, sikkerhed og grundlæggende rettigheder, og den sikrer fri bevægelighed for AI-baserede varer og tjenesteydelser på tværs af grænserne og forhindrer således medlemsstaterne i at indføre restriktioner for udvikling, markedsføring og anvendelse af AI-systemer, medmindre det udtrykkeligt er tilladt i henhold til denne forordning.
- (2) Systemer med kunstig intelligens (AI-systemer) kan nemt anvendes i flere sektorer af økonomien og i samfundet, herunder på tværs af grænserne, og cirkulere i hele Unionen. Visse medlemsstater har allerede undersøgt muligheden for nationale regler til sikring af, at kunstig intelligens er sikker, og at den udvikles og anvendes i overensstemmelse med forpligtelserne vedrørende grundlæggende rettigheder. Forskellige nationale regler kan føre til fragmentering af det indre marked og mindske retssikkerheden for operatører, der udvikler eller anvender AI-systemer. Der bør derfor sikres et ensartet og højt beskyttelsesniveau i hele Unionen, samtidig med at forskelle, der hæmmer den frie bevægelighed for AI-systemer og relaterede produkter og tjenesteydelser på det indre marked, bør forhindres ved at fastsætte ensartede forpligtelser for operatører og garantere en ensartet beskyttelse af tvingende almene hensyn og personers rettigheder i hele det indre marked på grundlag af artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF). For så vidt som denne

<sup>31</sup> EUT C [...] af [...], s. [...].

<sup>32</sup> EUT C [...] af [...], s. [...].

forordning indeholder specifikke regler om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger vedrørende begrænsninger i anvendelsen af AI-systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse, er det desuden hensigtsmæssigt at basere denne forordning på artikel 16 i TEUF for så vidt angår disse specifikke regler. I lyset af disse specifikke regler og anvendelsen af artikel 16 i TEUF bør Det Europæiske Databeskyttelsesråd høres.

- (3) Kunstig intelligens er en vifte af teknologier i hurtig udvikling, som kan bidrage til brede økonomiske og samfundsmæssige fordele på tværs af hele spektret af industrier og sociale aktiviteter. Ved at forbedre prognoser, optimere operationer og ressourceallokering og personalisere de digitale løsninger, der er tilgængelige for enkeltpersoner og organisationer, kan anvendelsen af kunstig intelligens give virksomheder vigtige konkurrencemæssige fordele og fremme socialt og miljømæssigt gavnlige resultater, f.eks. inden for sundhedspleje, landbrug, uddannelse, infrastrukturforvaltning, energi, transport og logistik, offentlige tjenester, sikkerhed, retsvæsen, ressource- og energieffektivitet samt modvirkning af og tilpasning til klimaændringer.
- (4) Samtidig kan kunstig intelligens, afhængigt af omstændighederne med hensyn til dens specifikke anvendelse, skabe risici og skade offentlige interesser og rettigheder, der er beskyttet af EU-retten. Sådant skade kan være af materiel eller immateriel karakter.
- (5) Der er derfor behov for en EU-retlig ramme, der fastsætter harmoniserede regler for kunstig intelligens, for at fremme udviklingen, anvendelsen og udbredelsen af kunstig intelligens på det indre marked, som samtidig opfylder et højt beskyttelsesniveau for offentlige interesser, såsom sundhed og sikkerhed og beskyttelse af grundlæggende rettigheder, som anerkendt og beskyttet i EU-retten. For at nå dette mål bør der fastsættes regler for markedsføring og ibrugtagning af visse AI-systemer for at sikre et velfungerende indre marked og give disse systemer mulighed for at drage fordel af princippet om fri bevægelighed for varer og tjenesteydelser. Med fastsættelse af reglerne i denne forordning støttes målet om, at Unionen skal være førende på verdensplan inden for udvikling af sikker, pålidelig og etisk kunstig intelligens som anført af Det Europæiske Råd<sup>33</sup>, og der sikres beskyttelse af etiske principper, som Europa-Parlamentet specifikt har anmodet om<sup>34</sup>.
- (6) Begrebet AI-system bør defineres klart for at sikre retssikkerheden og samtidig være fleksibelt nok til at tage højde for den fremtidige teknologiske udvikling. Definitionen bør baseres på softwarens vigtigste funktionelle karakteristika, navnlig evnen til for et givet sæt mål, der er fastsat af mennesker, at generere output såsom indhold, forudsigelser, anbefalinger eller beslutninger, der påvirker det miljø, som systemet interagerer med, hvad enten det er i en fysisk eller digital dimension. AI-systemer kan udformes med henblik på at fungere med varierende grader af autonomi og kan anvendes selvstændigt eller som en del af et produkt, uanset om systemet er fysisk integreret i produktet (indlejret) eller tjener produktets funktionalitet uden at være integreret deri (ikke indlejret). Definitionen af et AI-system bør suppleres med en liste over specifikke teknikker og tilgange, der anvendes i dets udvikling, og som bør

---

<sup>33</sup> Det Europæiske Råd, Ekstraordinært møde i Det Europæiske Råd (1. og 2. oktober 2020) – Konklusioner, EUCO 13/20, 2020, s. 6.

<sup>34</sup> Europa-Parlamentets beslutning af 20. oktober 2020 med henstillinger til Kommissionen om en ramme for etiske aspekter af kunstig intelligens, robotteknologi og relaterede teknologier, 2020/2012(INL).

holdes ajour i lyset af den markedsmæssige og teknologiske udvikling gennem Kommissionens vedtagelse af delegerede retsakter med henblik på at ændre denne liste.

- (7) Begrebet biometriske data, der anvendes i denne forordning, er i overensstemmelse med og bør fortolkes i overensstemmelse med begrebet biometriske data som defineret i artikel 4, stk. 14, i Europa-Parlamentets og Rådets forordning (EU) 2016/679<sup>35</sup>, artikel 3, stk. 18, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725<sup>36</sup> og artikel 3, stk. 13, i Europa-Parlamentets og Rådets direktiv (EU) 2016/680<sup>37</sup>.
- (8) Begrebet "system til biometrisk fjernidentifikation" som anvendt i denne forordning bør defineres funktionelt som et AI-system, der har til formål at identificere fysiske personer på afstand ved at sammenligne en persons biometriske data med de biometriske data i en referencedatabase, uden forudgående viden om, hvorvidt målpersonen vil være til stede og kan identificeres, uanset hvilken teknologi, hvilke processer eller hvilke typer biometriske data der anvendes. I betragtning af deres forskellige karakteristika og måder, hvorpå de anvendes, samt de forskellige risici, der er forbundet hermed, bør der skelnes mellem "systemer til biometrisk fjernidentifikation i realtid" og "systemer til efterfølgende biometrisk fjernidentifikation". Hvis der er tale om realtidssystemer, sker optagelsen af de biometriske data, sammenligningen og identifikationen øjeblikkeligt, næsten øjeblikkeligt eller under alle omstændigheder uden væsentlig forsinkelse. I denne forbindelse bør der ikke være mulighed for at omgå denne forordnings bestemmelser om realtidsanvendelse af de pågældende AI-systemer ved at tilføje mindre forsinkelser. Realtidssystemer omfatter anvendelse af direkte eller lettere forskudt materiale såsom videooptagelser, der genereres af et kamera eller en anden anordning med tilsvarende funktioner. Er der derimod tale om systemer til efterfølgende biometrisk fjernidentifikation, optages de biometriske data, og først efter en betydelig forsinkelse finder sammenligningen og identifikationen sted. Der er tale om materiale, såsom billeder eller videooptagelser, der genereres af videoovervågningskameraer eller private enheder, og som er frembragt inden systemets anvendelse for så vidt angår de pågældende fysiske personer.
- (9) I denne forordning bør begrebet offentlige steder forstås som ethvert fysisk sted, der er tilgængeligt for offentligheden, uanset om det pågældende sted er privatejet eller offentligt ejet. Begrebet omfatter derfor ikke steder af privat karakter, som normalt ikke er frit tilgængelige for tredjeparter, herunder retshåndhævende myndigheder, medmindre disse parter er blevet specifikt inviteret eller bemyndiget, såsom boliger, private klubber, kontorer, lagerbygninger og fabrikker. Online steder er heller ikke

---

<sup>35</sup> Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

<sup>36</sup> Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

<sup>37</sup> Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (retshåndhævelsesdirektivet) (EUT L 119 af 4.5.2016, s. 89).

omfattet, da der ikke er tale om fysiske steder. Det forhold, at der kan være visse betingelser for adgang til et bestemt sted, såsom entrébilletter eller aldersbegrænsninger, betyder imidlertid ikke i sig selv, at stedet ikke er offentligt som defineret i denne forordning. Ud over offentlige steder som gader, relevante dele af offentlige bygninger og de fleste transportinfrastrukturer er steder som f.eks. biografteatre, butikker og indkøbscentre derfor normalt også offentlige. Om et givet sted betragtes som offentligt, bør imidlertid afgøres fra sag til sag under hensyntagen til de særlige forhold i den enkelte situation.

- (10) For at sikre lige vilkår og en effektiv beskyttelse af fysiske personers rettigheder og friheder i hele Unionen bør de regler, der fastsættes ved denne forordning, finde anvendelse på udbydere af AI-systemer på en ikkediskriminerende måde, uanset om de er etableret i Unionen eller i et tredjeland, og på brugere af AI-systemer, der er etablerede i Unionen.
- (11) I betragtning af deres digitale karakter bør visse AI-systemer være omfattet af denne forordnings anvendelsesområde, selv om de hverken bringes i omsætning, ibrugtages eller anvendes i Unionen. Dette er f.eks. tilfældet for en operatør, der er etableret i Unionen, og som indgår kontrakter om visse tjenesteydelser med en operatør, der er etableret uden for Unionen, i forbindelse med en aktivitet, der skal udføres af et AI-system, der kan betegnes som højrisiko, og som har virkninger for fysiske personer i Unionen. Under disse omstændigheder kunne det AI-system, der anvendes af operatøren uden for Unionen, behandle data, der lovligt er indsamlet i og overført fra Unionen, og levere outputtet fra dette AI-systems behandling til den kontraherende operatør i Unionen, uden at dette AI-system bringes i omsætning, ibrugtages eller anvendes i Unionen. For at forhindre omgåelse af denne forordning og sikre en effektiv beskyttelse af fysiske personer i Unionen, bør denne forordning også finde anvendelse på udbydere og brugere af AI-systemer, der er etableret i et tredjeland, i det omfang det output, der produceres af disse systemer, anvendes i Unionen. For at tage hensyn til eksisterende ordninger og særlige behov for samarbejde med udenlandske partnere, med hvem der udveksles oplysninger og bevismateriale, bør denne forordning ikke finde anvendelse på offentlige myndigheder i et tredjeland og internationale organisationer, når disse handler inden for rammerne af internationale aftaler indgået på nationalt eller europæisk plan om retshåndhævelse og retligt samarbejde med Unionen eller med dens medlemsstater. Sådanne aftaler er indgået bilateralt mellem medlemsstaterne og tredjelande eller mellem Den Europæiske Union, Europol og andre EU-agenturer og tredjelande og internationale organisationer.
- (12) Denne forordning bør også finde anvendelse på Unionens institutioner, kontorer, organer og agenturer, når de fungerer som udbyder eller bruger af et AI-system. AI-systemer, der udelukkende udvikles eller anvendes til militære formål, bør ikke omfattes af denne forordnings anvendelsesområde, hvis anvendelsen henhører under den fælles udenrigs- og sikkerhedspolitik, der er reguleret i afsnit V i traktaten om Den Europæiske Union (TEU). Denne forordning berører ikke bestemmelserne om formidleransvar for tjenesteydere i Europa-Parlamentets og Rådets direktiv 2000/31/EF [som ændret ved retsakten om digitale tjenester].
- (13) For at sikre et ensartet højt beskyttelsesniveau for offentlige interesser med hensyn til sundhed, sikkerhed og grundlæggende rettigheder bør der fastsættes fælles normgivende standarder for alle højrisiko-AI-systemer. Disse standarder bør være i overensstemmelse med Den Europæiske Unions charter om grundlæggende rettigheder (chartret) og bør være ikke-diskriminerende og i overensstemmelse med Unionens internationale handelsforpligtelser.

- (14) For at indføre et proportionalt og effektivt sæt bindende regler for AI-systemer bør der anvendes en klart defineret risikobaseret tilgang. Denne tilgang bør tilpasse typen og indholdet af sådanne regler til graden og omfanget af de risici, som AI-systemer kan generere. Det er derfor nødvendigt at forbyde visse former for praksis med hensyn til kunstig intelligens, at fastsætte krav til højrisiko-AI-systemer og forpligtelser for de relevante operatører og at fastsætte gennemsigthedsforpligtelser for visse AI-systemer.
- (15) Ud over de mange nyttige anvendelser af kunstig intelligens kan teknologien også misbruges og resultere i nye og effektive værktøjer til manipulativ, udnyttende og socialt kontrollerende praksis. Sådanne praksis er særlig skadelig og bør forbydes, fordi den er i modstrid med Unionens værdier om respekt for menneskelig værdighed, frihed, ligestilling, demokrati og retsstatsprincippet og med Unionens grundlæggende rettigheder, herunder retten til beskyttelse mod forskelsbehandling, retten til databeskyttelse, retten til privatlivets fred og børns rettigheder.
- (16) Omsætning, ibrugtagning eller anvendelse af visse AI-systemer, der har til formål at forvride menneskers adfærd, og hvor der er sandsynlighed for fysiske eller psykiske skader, bør forbydes. Sådanne AI-systemer anvender subliminale komponenter, som mennesker ikke kan opfatte, eller de udnytter børns og voksnes sårbarheder på baggrund af alder eller fysisk eller mentalt handicap. De gør dette med den hensigt i væsentlig grad at forvride en persons adfærd og på en måde, der forvolder eller sandsynligvis vil forvolde den pågældende eller en anden person skade. Hensigten kan ikke formodes, hvis forvrængningen af menneskelig adfærd skyldes faktorer, som ligger uden for AI-systemet og uden for udbyderens eller brugerens kontrol. Legitim forskning i forbindelse med sådanne AI-systemer bør ikke hæmmes af forbuddet, hvis sådan forskning ikke anvender AI-systemet i forholdet mellem menneske og maskine på en måde, som udsætter fysiske personer for skade, og hvis sådan forskning udføres i overensstemmelse med anerkendte etiske standarder for videnskabelig forskning.
- (17) AI-systemer, der af offentlige myndigheder eller på deres vegne gør generel brug af sociale pointsystemer på fysiske personer, kan føre til diskriminerende resultater og udelukkelse af visse grupper. De kan dermed krænke retten til værdighed og retten til beskyttelse mod forskelsbehandling og værdierne lighed og retfærdighed. Sådanne AI-systemer evaluerer eller klassificerer fysiske personers troværdighed på grundlag af deres sociale adfærd i flere sammenhænge eller kendte eller forudsagte personlige egenskaber eller personlighedstræk. Det sociale pointsystem, der anvendes i sådanne AI-systemer, kan føre til en skadelig eller ugunstig behandling af fysiske personer eller hele grupper heraf i sociale sammenhænge, som ikke har noget at gøre med den sammenhæng, i hvilken dataene oprindeligt blev genereret eller indsamlet, eller til en skadelig behandling, der er uforholdsmæssig eller uberettiget i forhold til alvoren af deres sociale adfærd. Sådanne AI-systemer bør derfor forbydes.
- (18) Anvendelsen af AI-systemer til biometrisk fjernidentifikation i realtid af fysiske personer på offentlige steder med henblik på retshåndhævelse anses for at være særligt indgribende i de berørte personers rettigheder og friheder, for så vidt som det kan påvirke privatlivets fred for en stor del af befolkningen, skabe en følelse af konstant overvågning og indirekte afskrække fra udøvelsen af forsamlingsfriheden og andre grundlæggende rettigheder. Desuden indebærer den øjeblikkelige virkning og de begrænsede muligheder for yderligere kontrol eller justeringer i forbindelse med anvendelsen af systemer, der fungerer i realtid, øgede risici for rettigheder og friheder for de personer, der er berørt af retshåndhævelsesaktiviteterne.



- (19) Anvendelsen af disse systemer med henblik på retshåndhævelse bør derfor forbydes, undtagen i tre udtømmende opregnede og snævert definerede situationer, hvor anvendelsen er strengt nødvendig for at opfylde en væsentlig samfundsinteresse, hvis betydning vejer tungere end risiciene. Disse situationer omfatter eftersøgning af potentielle ofre for kriminalitet, herunder forsvundne børn, visse trusler mod fysiske personers liv eller fysiske sikkerhed eller om et terrorangreb, samt afsløring, lokalisering, identifikation eller retsforfølgning af gerningsmænd, der har begået, eller af personer, der mistænkes for at have begået, strafbare handlinger, der er omhandlet i Rådets rammeafgørelse 2002/584/JHA<sup>38</sup>, og som i den pågældende medlemsstat kan straffes med frihedsstraf eller en anden frihedsberøvende foranstaltning af en maksimal varighed på mindst tre år som fastsat i denne medlemsstats lovgivning. En sådan tærskel for frihedsstraf eller anden frihedsberøvende foranstaltning i overensstemmelse med national ret bidrager til at sikre, at lovovertredelsen er af tilstrækkelig alvorlig karakter til potentielt at berettige anvendelsen af systemer til biometrisk fjernidentifikation i realtid. Desuden er nogle af de 32 strafbare handlinger, der er opregnet i Rådets rammeafgørelse 2002/584/JHA, i praksis mere relevante end andre, idet anvendelsen af biometrisk fjernidentifikation i realtid sandsynligvis vil være nødvendig og rimelig i meget varierende grad for afsløring, lokalisering, identifikation eller retsforfølgning af en gerningsmand, der har begået, eller af en person, der mistænkes for at have begået, strafbare handlinger, der er opført på listen, og under hensyntagen til de sandsynlige forskelle i lovovertredelsens alvor, omfang eller mulige negative konsekvenser.
- (20) For at sikre, at disse systemer anvendes på en ansvarlig og rimelig måde, er det også vigtigt at fastslå, at der i hver af disse tre udtømmende opregnede og snævert definerede situationer bør tages hensyn til visse elementer, navnlig med hensyn til situationens karakter, som ligger til grund for anmodningen, og konsekvenserne af anvendelsen for alle berørte personers rettigheder og friheder samt de garantier og betingelser, der er fastsat for brugen. Anvendelsen af systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse bør desuden underlægges passende begrænsninger i tid og sted, navnlig med hensyn til beviser eller indikationer vedrørende truslerne, ofrene eller gerningsmanden. Referencedatabasen over personer bør være passende for hvert enkelt anvendelsestilfælde i hver af de tre ovennævnte situationer.
- (21) Enhver anvendelse af et system til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse bør være betinget af en udtrykkelig og specifik tilladelse fra en judiciel myndighed eller en uafhængig administrativ myndighed i en medlemsstat. En sådan tilladelse bør i princippet indhentes forud for anvendelsen, undtagen i behørigt begrundede hastende tilfælde, dvs. situationer, hvor behovet for at anvende de pågældende systemer er af en sådan art, at det er praktisk og objektivt umuligt at opnå en tilladelse, inden anvendelsen påbegyndes. I sådanne hastende situationer bør anvendelsen begrænses til det absolut nødvendige minimum og være underlagt passende garantier og betingelser som fastsat i national ret og præciseret af den retshåndhævende myndighed selv i forbindelse med hver enkelt hastesag. Desuden bør den retshåndhævende myndighed i sådanne situationer søge at opnå en tilladelse så hurtigt som muligt og samtidig begrunde, hvorfor den ikke har været i stand til at anmode om den tidligere.

---

<sup>38</sup> Rådets rammeafgørelse 2002/584/RIA af 13. juni 2002 om den europæiske arrestordre og om procedurerne for overgivelse mellem medlemsstaterne (EFT L 190 af 18.7.2002, s. 1).

- (22) Endvidere bør det inden for denne forordnings udtømmende rammer fastsættes, at en sådan anvendelse på en medlemsstats område i overensstemmelse med denne forordning kun bør være mulig, hvis og i det omfang den pågældende medlemsstat har besluttet udtrykkeligt at give mulighed for at tillade en sådan anvendelse i sine detaljerede bestemmelser i national ret. Det står derfor medlemsstaterne frit for i henhold til denne forordning slet ikke at fastsætte en sådan mulighed eller kun at fastsætte en sådan mulighed med hensyn til nogle af de forhold, der i henhold til denne forordning kan begrunde en godkendt anvendelse.
- (23) Anvendelsen af AI-systemer til biometrisk fjernidentifikation i realtid af fysiske personer på offentlige steder med henblik på retshåndhævelse indebærer nødvendigvis behandling af biometriske data. De bestemmelser i denne forordning, der med forbehold af visse undtagelser forbyder en sådan anvendelse, der er baseret på artikel 16 i TEUF, bør finde anvendelse som *lex specialis* for så vidt angår reglerne om behandling af biometriske data i artikel 10 i direktiv (EU) 2016/680 og således regulere anvendelsen og behandlingen af biometriske data på en udtømmende måde. En sådan anvendelse og behandling bør derfor kun være mulig i det omfang, det er foreneligt med den ramme, der er fastsat i denne forordning, uden at der uden for denne ramme er mulighed for, at de kompetente myndigheder, når de handler med henblik på retshåndhævelse, kan anvende sådanne systemer og i forbindelse hermed behandle sådanne data af de grunde, der er anført i artikel 10 i direktiv (EU) 2016/680. I denne sammenhæng har denne forordning ikke til formål at tilvejebringe retsgrundlaget for behandling af personoplysninger i henhold til artikel 8 i direktiv 2016/680. Anvendelsen af systemer til biometrisk fjernidentifikation i realtid på offentlige steder til andre formål end retshåndhævelse, herunder af kompetente myndigheder, bør imidlertid ikke være omfattet af den specifikke ramme for en sådan anvendelse med henblik på retshåndhævelse som fastsat i denne forordning. En sådan anvendelse til andre formål end retshåndhævelse bør derfor ikke være underlagt kravet om en tilladelse i henhold til denne forordning og de gældende detaljerede bestemmelser i national ret, der kan give den virkning.
- (24) Enhver behandling af biometriske data og andre personoplysninger, der benyttes i forbindelse med anvendelsen af AI-systemer til biometrisk identifikation, undtagen i forbindelse med anvendelsen af systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse som reguleret ved denne forordning, herunder når disse systemer anvendes af kompetente myndigheder på offentlige steder til andre formål end retshåndhævelse, bør fortsat opfylde alle krav, der følger af artikel 9, stk. 1, i forordning (EU) 2016/679, artikel 10, stk. 1, i forordning (EU) 2018/1725 og artikel 10 i direktiv (EU) 2016/680, alt efter hvad der er relevant.
- (25) I medfør af artikel 6a i protokol nr. 21 om Det Forenede Kongeriges og Irlands stilling, for så vidt angår området med frihed, sikkerhed og retfærdighed, der er knyttet som bilag til TEU og TEUF, er Irland ikke bundet af regler fastsat i artikel 5, stk. 1, litra d), stk. 2 og stk. 3 i denne forordning, der er vedtaget på grundlag af artikel 16 i TEUF vedrørende medlemsstaternes behandling af personoplysninger under udøvelsen af aktiviteter, der er omfattet af tredje del, afsnit V, kapitel 4 eller 5, i TEUF, når Irland ikke er bundet af regler vedrørende former for strafferetligt samarbejde eller politisamarbejde, der kræver overholdelse af de bestemmelser, der er fastsat på grundlag af artikel 16 i TEUF.
- (26) I medfør af artikel 2 og 2a i protokol nr. 22 om Danmarks stilling, der er knyttet som bilag til TEU og TEUF, er de regler, der er fastsat i artikel 5, stk. 1, litra d), stk. 2 og stk. 3 i denne forordning, der er vedtaget på grundlag af artikel 16 i TEUF vedrørende

medlemsstaternes behandling af personoplysninger under udøvelsen af aktiviteter, der er omfattet af tredje del, afsnit V, kapitel 4 eller 5, i TEUF, ikke bindende for og finder ikke anvendelse i Danmark.

- (27) Højrisiko-AI-systemer bør kun bringes i omsætning på EU-markedet eller tages i brug, hvis de opfylder visse obligatoriske krav. Disse krav bør sikre, at højrisiko-AI-systemer, der er tilgængelige i Unionen, eller hvis output på anden måde anvendes i Unionen, ikke udgør uacceptable risici for vigtige offentlige interesser i Unionen som anerkendt og beskyttet i EU-retten. AI-systemer, der er identificeret som indebærende høj risiko, bør begrænses til systemer, der har en betydelig skadelig indvirkning på menneskers sundhed, sikkerhed og grundlæggende rettigheder i Unionen, og sådanne begrænsninger minimerer eventuelle potentielle restriktioner for den internationale handel.
- (28) AI-systemer kan forårsage negative virkninger for menneskers sundhed og sikkerhed, navnlig når sådanne systemer fungerer som produktkomponenter. I overensstemmelse med målene for EU-harmoniseringslovgivningen om at lette den frie bevægelighed for produkter i det indre marked og sørge for, at kun sikre produkter, der opfylder kravene, kommer ind på markedet, er det vigtigt, at de sikkerhedsrisici, som et produkt som helhed kan udgøre på grund af dets digitale komponenter, herunder AI-systemer, behørigt forebygges og afbødes. F.eks. bør stadig mere autonome robotter, hvad enten det er i forbindelse med fremstilling eller personlig bistand og pleje, være i stand til at operere sikkert og udføre deres funktioner i komplekse miljøer. Også i sundhedssektoren, hvor det drejer sig direkte om liv og sundhed, bør stadig mere avancerede diagnosesystemer og systemer, der understøtter menneskers beslutninger, være pålidelige og nøjagtige. Omfanget af et AI-systems negative indvirkning på de grundlæggende rettigheder, der er beskyttet af chartret, er særlig relevant, når et AI-system klassificeres som et højrisikosystem. Disse rettigheder omfatter retten til menneskelig værdighed, respekt for privatliv og familieliv, beskyttelse af personoplysninger, ytrings- og informationsfrihed, forsamlings- og foreningsfrihed og ikkeforskelsbehandling, forbrugerbeskyttelse, arbejdstagerrettigheder, rettigheder for personer med handicap, adgang til effektive retsmidler og til en retfærdig rettergang, retten til et forsvar og uskyldsformodningen samt retten til god forvaltning. Ud over disse rettigheder er det vigtigt at fremhæve, at børn har specifikke rettigheder som fastsat i artikel 24 i EU's charter og i De Forenede Nationers konvention om barnets rettigheder (yderligere uddybet i FN's børnekonvention, generel bemærkning nr. 25 vedrørende det digitale miljø), som begge kræver, at der tages hensyn til børns sårbarhed, og at der ydes den beskyttelse og omsorg, der er nødvendig for deres trivsel. Den grundlæggende ret til et højt miljøbeskyttelsesniveau, der er nedfældet i chartret og gennemført i Unionens politikker, bør også tages i betragtning ved vurderingen af alvoren af den skade, som et AI-system kan forårsage, herunder i forbindelse med menneskers sundhed og sikkerhed.
- (29) For så vidt angår højrisiko-AI-systemer, der er sikkerhedskomponenter i produkter eller systemer, eller som selv er produkter eller systemer, der er omfattet af anvendelsesområdet for Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008<sup>39</sup>, Europa-Parlamentets og Rådets forordning (EU) nr. 167/2013<sup>40</sup>, Europa-

---

<sup>39</sup> Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 af 11. marts 2008 om fælles bestemmelser om sikkerhed inden for civil luftfart og om ophævelse af forordning (EF) nr. 2320/2002 (EUT L 97 af 9.4.2008, s. 72).

Parlamentets og Rådets forordning (EU) nr. 168/2013<sup>41</sup>, Europa-Parlamentets og Rådets direktiv 2014/90/EU<sup>42</sup>, Europa-Parlamentets og Rådets direktiv (EU) 2016/797<sup>43</sup>, Europa-Parlamentets og Rådets forordning (EU) 2018/858<sup>44</sup>, Europa-Parlamentets og Rådets forordning (EU) 2018/1139<sup>45</sup> og Europa-Parlamentets og Rådets forordning (EU) 2019/2144<sup>46</sup>, bør disse retsakter ændres for at sikre, at Kommissionen, på grundlag af de særlige tekniske og reguleringsmæssige forhold i hver enkelt sektor og uden at intervenere i de eksisterende forvaltnings-, overensstemmelsesvurderings- og håndhævelsesmekanismer og de myndigheder, der er fastsat heri, tager hensyn til de obligatoriske krav til højrisiko-AI-systemer, der er fastsat i denne forordning, når den vedtager relevante fremtidige delegerede retsakter eller gennemførelsesretsakter på grundlag af disse retsakter.

- (30) For så vidt angår AI-systemer, der er sikkerhedskomponenter i produkter, eller som selv er produkter, der er omfattet af anvendelsesområdet for visse EU-harmoniseringsretsakter, er det hensigtsmæssigt at klassificere dem som højrisikosystemer i henhold til denne forordning, hvis det pågældende produkt overensstemmelsesvurderes af en tredjeparts overensstemmelsesvurderingsorgan i henhold til den relevante EU-harmoniseringslovgivning. Sådanne produkter er navnlig maskiner, legetøj, elevatorer, materiel og sikringsystemer til anvendelse i eksplosionsfarlig atmosfære, radioudstyr, trykudstyr, udstyr til fritidsfartøjer, tovbaneanlæg, gasapparater, medicinsk udstyr og in vitro-diagnostisk medicinsk udstyr.
- (31) Klassificeringen af et AI-system som et højrisikosystem i henhold til denne forordning bør ikke nødvendigvis betyde, at det produkt, hvori AI-systemet indgår som sikkerhedskomponent, eller selve AI-systemet, når det betragtes som et produkt, anses for at have høj risiko i henhold til de kriterier, der er fastsat i den relevante EU-harmoniseringslovgivning, der finder anvendelse på produktet. Dette er navnlig

---

<sup>40</sup> Europa-Parlamentets og Rådets forordning (EU) nr. 167/2013 af 5. februar 2013 om godkendelse og markedsovervågning af landbrugs- og skovbrugstraktorer (EUT L 60 af 2.3.2013, s. 1).

<sup>41</sup> Europa-Parlamentets og Rådets forordning (EU) nr. 168/2013 af 15. januar 2013 om godkendelse og markedsovervågning af to- og trehjulede køretøjer samt quadricykler (EUT L 60 af 2.3.2013, s. 52).

<sup>42</sup> Europa-Parlamentets og Rådets direktiv 2014/90/EU af 23. juli 2014 om skibsudstyr og om ophævelse af Rådets direktiv 96/98/EF (EUT L 257 af 28.8.2014, s. 146).

<sup>43</sup> Europa-Parlamentets og Rådets direktiv (EU) 2016/797 af 11. maj 2016 om interoperabilitet i jernbanesystemet i Den Europæiske Union (EUT L 138 af 26.5.2016, s. 44).

<sup>44</sup> Europa-Parlamentets og Rådets forordning (EU) 2018/858 af 30. maj 2018 om godkendelse og markedsovervågning af motorkøretøjer og påhængskøretøjer dertil samt af systemer, komponenter og separate tekniske enheder til sådanne køretøjer, om ændring af forordning (EF) nr. 715/2007 og (EF) nr. 595/2009 og om ophævelse af direktiv 2007/46/EF (EUT L 151 af 14.6.2018, s. 1).

<sup>45</sup> Europa-Parlamentets og Rådets forordning (EU) 2018/1139 af 4. juli 2018 om fælles regler for civil luftfart og oprettelse af Den Europæiske Unions Luftfartssikkerhedsagentur og om ændring af forordning (EF) nr. 2111/2005, (EF) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 og direktiv 2014/30/EU og 2014/53/EU og om ophævelse af (EF) nr. 552/2004 og (EF) nr. 216/2008 og Rådets forordning (EØF) nr. 3922/91 (EUT L 212 af 22.8.2018, s. 1).

<sup>46</sup> Europa-Parlamentets og Rådets forordning (EU) 2019/2144 af 27. november 2019 om krav til typegodkendelse af motorkøretøjer og påhængskøretøjer dertil samt systemer, komponenter og separate tekniske enheder til sådanne køretøjer for så vidt angår deres generelle sikkerhed og beskyttelsen af køretøjspassagerer og bløde trafikanter og om ændring af Europa-Parlamentets og Rådets forordning (EU) 2018/858 og ophævelse af Europa-Parlamentets og Rådets forordning (EF) nr. 78/2009, (EF) nr. 79/2009 og (EF) nr. 661/2009 og Kommissionens forordning (EF) 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 og (EU) 2015/166 (EUT L 325 af 16.12.2019, s. 1).

tilfældet med Europa-Parlamentets og Rådets forordning (EU) 2017/745<sup>47</sup> og Europa-Parlamentets og Rådets forordning (EU) 2017/746<sup>48</sup>, hvor en tredjepart foretager overensstemmelsesvurderinger af mellemrisiko- og højrisikoprodukter.

- (32) Selvstændige AI-systemer, dvs. andre højrisiko-AI-systemer end dem, der er sikkerhedskomponenter i produkter, eller som selv er produkter, bør klassificeres som højrisikosystemer, hvis de set i lyset af deres tilsigtede formål udgør en høj risiko for skade på menneskers sundhed og sikkerhed eller grundlæggende rettigheder, idet der tages hensyn til både sandsynligheden for den mulige skade og dens alvorlighed, og hvis de anvendes på en række specifikt foruddefinerede områder, der er angivet i forordningen. Disse systemer udpeges ved hjælp af den samme metode og ud fra de samme kriterier som i forbindelse med eventuelle fremtidige ændringer af listen over højrisiko-AI-systemer.
- (33) Tekniske unøjagtigheder i AI-systemer, der er beregnet til biometrisk fjernidentifikation af fysiske personer, kan føre til skæve resultater og have diskriminerende virkning. Det gælder særligt med hensyn til alder, etnicitet, køn og handicap. Derfor bør systemer til biometrisk fjernidentifikation i realtid og efterfølgende biometrisk fjernidentifikation klassificeres som højrisikosystemer. I betragtning af de risici, systemerne udgør, bør begge typer af systemer til biometrisk fjernidentifikation være underlagt specifikke krav med hensyn til logningskapacitet og menneskeligt tilsyn.
- (34) For så vidt angår forvaltning og drift af kritisk infrastruktur bør AI-systemer, der er beregnet til anvendelse som sikkerhedskomponenter i forvaltningen og driften af vejtrafik og forsyning af vand, gas, varme og elektricitet, klassificeres som højrisikosystemer, da svigt eller funktionsfejl i disse systemer kan bringe menneskers liv og sundhed i fare i stort omfang og føre til betydelige forstyrrelser i de sociale og økonomiske aktiviteter.
- (35) AI-systemer, der anvendes inden for uddannelse eller erhvervsuddannelse, navnlig til optagelse eller fordeling af personer på uddannelsesinstitutioner eller til at evaluere personer i forbindelse med prøver som en del af eller som en forudsætning for deres uddannelse, bør betragtes som højrisikosystemer, da de kan afgøre menneskers uddannelsesmæssige og arbejdsmæssige livsforløb og dermed påvirke deres evne til at sikre sig et livsgrundlag. Hvis sådanne systemer udformes og anvendes forkert, kan de krænke retten til uddannelse og retten til ikke at blive forskelsbehandlet samt opretholde historiske diskriminationsmønstre.
- (36) AI-systemer, der anvendes inden for beskæftigelse, forvaltning af arbejdskraft og adgang til selvstændig erhvervsvirksomhed, navnlig til rekruttering og udvælgelse af personer og til beslutningstagning om forfremmelse og afskedigelse og til opgavefordeling, overvågning og evaluering af personer i arbejdsmæssige kontraktforhold, bør også klassificeres som højrisikosystemer, da de kan påvirke menneskers fremtidige karrieremuligheder og livsgrundlag betydeligt. De relevante arbejdsmæssige kontraktforhold bør omfatte ansatte og personer, der leverer

---

<sup>47</sup> Europa-Parlamentets og Rådets forordning (EU) 2017/745 af 5. april 2017 om medicinsk udstyr, om ændring af direktiv 2001/83/EF, forordning (EF) nr. 178/2002 og forordning (EF) nr. 1223/2009 og om ophævelse af Rådets direktiv 90/385/EØF og 93/42/EØF (EUT L 117 af 5.5.2017, s. 1).

<sup>48</sup> Europa-Parlamentets og Rådets forordning (EU) 2017/746 af 5. april 2017 om medicinsk udstyr til in vitro-diagnostik og om ophævelse af direktiv 98/79/EF og Kommissionens afgørelse 2010/227/EU (EUT L 117 af 5.5.2017, s. 176).

tjenesteydelser via platforme som omhandlet i Kommissionens arbejdsprogram for 2021. Sådanne personer bør i princippet ikke betragtes som brugere som defineret i denne forordning. Gennem hele rekrutteringsprocessen og i forbindelse med evaluering, forfremmelse eller fastholdelse af personer i arbejdsmæssige kontraktforhold kan sådanne systemer opretholde historiske diskriminationsmønstre, f.eks. mod kvinder, bestemte aldersgrupper, personer med handicap eller personer af bestemt racemæssig eller etnisk oprindelse eller med en bestemt seksuel orientering. AI-systemer, der anvendes til at overvåge disse personers præstationer og adfærd, kan også påvirke deres ret til databeskyttelse og ret til privatlivets fred.

- (37) Et andet område, hvor anvendelsen af AI-systemer kræver særlig opmærksomhed, er adgangen til og benyttelsen af visse væsentlige private og offentlige tjenester og de fordele, der er nødvendige for, at mennesker kan deltage fuldt ud i samfundet eller forbedre deres levestandard. Navnlig bør AI-systemer, der anvendes til at evaluere kreditvurderinger eller kreditværdigheden af fysiske personer, klassificeres som højrisiko-AI-systemer, da de afgør menneskers adgang til finansielle ressourcer eller væsentlige tjenester såsom bolig, elektricitet og telekommunikationstjenester. AI-systemer, der anvendes til dette formål, kan føre til forskelsbehandling af personer eller grupper og opretholde historiske diskriminationsmønstre, f.eks. på grundlag af racemæssig eller etnisk oprindelse, handicap, alder eller seksuel orientering, eller være med til at skabe nye former for diskriminerende virkninger. I betragtning af den meget begrænsede indvirkning og de alternativer, der er tilgængelige på markedet, bør AI-systemer, der anvendes i forbindelse med kreditvurderinger og vurdering af kreditværdighed, undtages, når de tages i brug af mindre udbydere til egen brug. Fysiske personer, der ansøger om eller modtager offentlige bistandsydelser og tjenester fra offentlige myndigheder, er typisk afhængige af sådanne ydelser og tjenester og befinder sig i en sårbar situation i forhold til de ansvarlige myndigheder. Hvis der anvendes AI-systemer til at afgøre, om der skal gives afslag på sådanne ydelser og tjenester, eller om de skal reduceres, ophæves eller tilbagekræves af myndighederne, kan systemerne have en betydelig indvirkning på menneskers livsgrundlag og krænke deres grundlæggende rettigheder såsom retten til social beskyttelse, ikkeforskelsbehandling, menneskelig værdighed eller adgang til effektive retsmidler. Sådanne systemer bør derfor klassificeres som højrisikosystemer. Ikke desto mindre bør denne forordning ikke hindre udviklingen eller anvendelsen af innovative tilgange i den offentlige forvaltning, som vil kunne drage fordel af en bredere anvendelse af AI-systemer, der er i overensstemmelse med reglerne og er sikre, forudsat at de ikke indebærer en høj risiko for juridiske og fysiske personer. Endelig bør AI-systemer, der anvendes til at sende beredskabstjenester i nødsituationer eller til at tildele prioriteter i forbindelse hermed, også klassificeres som højrisikosystemer, da de træffer beslutninger i situationer, der er meget kritiske for menneskers liv og sundhed og for deres ejendom.
- (38) Retshåndhævende myndigheders handlinger, der omfatter visse anvendelser af AI-systemer, er kendetegnet ved en betydelig ubalance i magtforholdet og kan føre til overvågning, anholdelse eller frihedsberøvelse af fysiske personer samt have andre negative indvirkninger på de grundlæggende rettigheder, der er sikret i chartret. Navnlig kan AI-systemer udvælge personer på diskriminerende eller på anden måde ukorrekt eller uretfærdig vis, hvis de ikke er trænet med data af høj kvalitet, ikke opfylder passende krav med hensyn til nøjagtighed og robusthed eller ikke er korrekt udformede og afprøvet, før de bringes i omsætning eller på anden måde tages i brug. Desuden kan udøvelsen af vigtige grundlæggende processuelle rettigheder såsom retten til adgang til effektive retsmidler, retten til en retfærdig rettergang og retten til et

forsvar samt uskyldsformodningen hindres, navnlig hvis sådanne AI-systemer ikke er tilstrækkeligt gennemsigtige, forklarlige og dokumenterede. Derfor bør en række AI-systemer, der er beregnet til anvendelse i retshåndhævelsesmæssig sammenhæng, hvor det er særlig vigtigt med nøjagtighed, pålidelighed og gennemsigtighed for at undgå negative virkninger, bevare offentlighedens tillid og sikre ansvarlighed og effektive retsmidler, klassificeres som højrisikosystemer. I betragtning af de pågældende aktiviteter karakter og de risici, der er forbundet med dem, bør disse højrisiko-AI-systemer navnlig omfatte AI-systemer, der er beregnet til at blive anvendt af retshåndhævende myndigheder til individuelle risikovurderinger, polygrafer og lignende værktøjer, påvisning af fysiske personers følelsesmæssige tilstand, afsløring af deepfake-indhold, vurdering af pålideligheden af bevismateriale i straffesager, forudsigelse af forekomsten eller gentagelsen af en faktisk eller potentiel strafbar handling ud fra profilering af fysiske personer, vurdering af fysiske personers eller grupper personlighedstræk og personlige egenskaber eller tidligere kriminelle adfærd, profilering i forbindelse med afsløring, efterforskning eller retsforfølgelse af strafbare handlinger samt kriminalanalyser vedrørende fysiske personer. AI-systemer, der specifikt er beregnet til skatte- og toldmyndigheders administrative procedurer, bør ikke betragtes som højrisiko-AI-systemer, der anvendes af retshåndhævende myndigheder med henblik på forebyggelse, afsløring, efterforskning og retsforfølgning af strafbare handlinger.

- (39) AI-systemer, der anvendes inden for migrationsstyring, asylforvaltning og grænsekontrol, berører personer, der ofte befinder sig i en særlig sårbar situation, og som er afhængige af resultatet af de kompetente offentlige myndigheders handlinger. I AI-systemer, der anvendes i disse sammenhænge, er nøjagtighed, gennemsigtighed og systemets ikkediskriminerende karakter derfor særlig vigtige med hensyn til at sikre, at de berørte personers grundlæggende rettigheder beskyttes, navnlig deres ret til fri bevægelighed, beskyttelse mod forskelsbehandling, beskyttelse af privatlivets fred og personoplysninger, international beskyttelse og god forvaltning. Derfor bør de AI-systemer, der er beregnet til at blive anvendt af de kompetente offentlige myndigheder, der er ansvarlige for opgaver inden for migrationsstyring, asylforvaltning og grænsekontrol, som polygrafer og lignende værktøjer eller til at påvise en fysisk persons følelsesmæssige tilstand, vurdere visse risici, som fysiske personer, der indrejser til en medlemsstats område eller ansøger om visum eller asyl, udgør, kontrollere ægtheden af fysiske personers relevante dokumenter, bistå de kompetente offentlige myndigheder i behandlingen af ansøgninger om asyl, visum og opholdstilladelse og hertil relaterede klager med henblik på at fastslå, om de fysiske personer, der ansøger, er berettigede, klassificeres som højrisikosystemer. AI-systemer, der anvendes inden for migrationsstyring, asylforvaltning og grænsekontrol, og som er omfattet af denne forordning, bør opfylde de relevante proceduremæssige krav i Europa-Parlamentets og Rådets direktiv 2013/32/EU<sup>49</sup>, Europa-Parlamentets og Rådets forordning (EF) nr. 810/2009<sup>50</sup> og anden relevant lovgivning.
- (40) Visse AI-systemer, der er beregnet til anvendelse inden for retspleje og i demokratiske processer, bør klassificeres som højrisikosystemer i betragtning af deres potentielt

---

<sup>49</sup> Europa-Parlamentets og Rådets direktiv 2013/32/EU af 26. juni 2013 om fælles procedurer for tildeling og fratagelse af international beskyttelse (EUT L 180 af 29.6.2013, s. 60).

<sup>50</sup> Europa-Parlamentets og Rådets forordning (EF) nr. 810/2009 af 13. juli 2009 om en fællesskabskodeks for visa (visumkodeks) (EUT L 243 af 15.9.2009, s. 1).

betydelige indvirkning på demokratiet, retsstatsprincippet, individets frihedsrettigheder samt retten til adgang til effektive retsmidler og retten til en retfærdig rettergang. Navnlig for at imødegå risikoen for forudindtaget, fejl og uigennemsigtighed bør de AI-systemer, der har til formål at bistå retlige myndigheder med at undersøge og fortolke fakta og lovgivningen og anvende lovgivningen i konkrete, faktuelle sager, klassificeres som højrisikosystemer. Denne kvalificering bør dog ikke omfatte AI-systemer, der er beregnet til rent supplerende administrative aktiviteter, som ikke har indflydelse på den egentlige retspleje i de enkelte sager, som f.eks. anonymisering eller pseudonymisering af retsafgørelser, dokumenter eller data, kommunikation mellem personale, administrative opgaver eller fordeling af ressourcer.

- (41) Klassificeringen af et AI-system som et højrisikosystem i henhold til denne forordning bør ikke fortolkes således, at anvendelsen af systemet nødvendigvis er lovlig i henhold til andre EU-retsakter eller national lovgivning, der er forenelig med EU-retten, f.eks. lovgivning om beskyttelse af personoplysninger, brug af polygrafer og lignende værktøjer eller andre systemer til at påvise fysiske personers følelsesmæssige tilstand. Enhver sådan anvendelse bør fortsat udelukkende ske i overensstemmelse med de gældende krav, der følger af chartret og de gældende afledte EU-retsfor skrifter og national ret. Denne forordning bør ikke forstås som et retsgrundlag for behandling af personoplysninger, herunder særlige kategorier af personoplysninger, hvor det er relevant.
- (42) For at begrænse risiciene fra højrisiko-AI-systemer, der bringes i omsætning eller på anden måde tages i brug på EU-markedet, for brugere og berørte personer bør der gælde visse obligatoriske krav under hensyntagen til det tilsigtede formål med anvendelsen af systemet og i overensstemmelse med det risikostyringssystem, som udbyderen skal indføre.
- (43) Der bør gælde krav for højrisiko-AI-systemer med hensyn til kvaliteten af de anvendte datasæt, teknisk dokumentation og registrering, gennemsigtighed og formidling af oplysninger til brugerne, menneskeligt tilsyn og robusthed, nøjagtighed og cybersikkerhed. Disse krav er nødvendige for effektivt at mindske risiciene for menneskers sundhed, sikkerhed og grundlæggende rettigheder, alt efter hvad der i lyset af systemets tilsigtede formål er relevant, og hvis foranstaltninger, der er mindre begrænsende for handelen, ikke er mulige, således at uberettigede handelsrestriktioner undgås.
- (44) Når det gælder om at sikre, at et højrisiko-AI-system yder efter hensigten og på sikker vis og ikke bliver en kilde til forskelsbehandling som forbudt i henhold til EU-retten, er en høj datakvalitet afgørende for mange AI-systemers ydeevne, navnlig hvis der gøres brug af teknikker, der omfatter træning af modeller. Trænings-, validerings- og prøvningsdatasæt af høj kvalitet kræver, at der indføres passende datastyrings- og dataforvaltningspraksisser. Trænings-, validerings- og prøvningsdatasættene bør være tilstrækkeligt relevante, repræsentative og fri for fejl og fuldstændige i forhold til systemets tilsigtede formål. De bør også have de relevante statistiske egenskaber, herunder med hensyn til de personer eller grupper af personer, på hvilke højrisiko-AI-systemet skal anvendes. Navnlig bør der i trænings-, validerings- og prøvningsdatasæt i det omfang, det er nødvendigt i lyset af deres tilsigtede formål, tages hensyn til de egenskaber, karakteristika eller elementer, der er særlige for den specifikke geografiske, adfærdsmæssige eller funktionelle ramme eller kontekst, inden for hvilken AI-systemet skal anvendes. For at sikre andres ret til beskyttelse mod den forskelsbehandling, der kan opstå som følge af skævheder i AI-systemer, bør udbydere



også kunne behandle særlige kategorier af personoplysninger for at sikre, at partiskhed i forbindelse med højrisiko-AI-systemer overvåges, opdages og korrigeres som et spørgsmål af væsentligt samfundshensyn.

- (45) Når der udvikles højrisiko-AI-systemer, bør visse aktører, som for eksempel udbydere, bemyndigede organer og andre relevante enheder såsom digitale innovationsknudepunkter, prøvnings- og forsøgsfaciliteter og forskere, have adgang til og kunne anvende datasæt af høj kvalitet inden for deres respektive aktivitetsområder, som er relateret til denne forordning. Fælles europæiske dataområder, som Kommissionen har oprettet, og fremme af datadeling mellem virksomheder og med myndigheder i almenhedens interesse vil være afgørende for at sikre pålidelig, ansvarlig og ikkediskriminerende adgang til data af høj kvalitet til træning, validering og prøvning af AI-systemer. På sundhedsområdet vil det europæiske sundhedsdataområde for eksempel fremme ikkediskriminerende adgang til sundhedsdata og træning af algoritmer med kunstig intelligens i disse datasæt på en måde, der beskytter privatlivets fred, er sikker, rettidig, gennemsigtig og pålidelig og underlagt en passende institutionel styring. Relevante kompetente myndigheder, herunder sektorspecifikke myndigheder, der giver eller understøtter adgang til data, kan også understøtte tilvejebringelsen af data af høj kvalitet til træning, validering og prøvning af AI-systemer.
- (46) Med hensyn til overholdelsen af kravene i denne forordning er det vigtigt, at der foreligger oplysninger om, hvordan højrisiko-AI-systemer er blevet udviklet, og hvordan de fungerer i hele deres livscyklus. Det kræver, at der føres fortegnelser og stilles en teknisk dokumentation til rådighed, som indeholder de oplysninger, der er nødvendige for at vurdere AI-systemets overensstemmelse med de relevante krav. Sådanne oplysninger bør omfatte systemets generelle egenskaber, kapacitet og begrænsninger samt algoritmer, data, trænings-, prøvnings- og valideringsprocesser foruden dokumentation for det relevante risikostyringssystem. Den tekniske dokumentation skal holdes ajour.
- (47) For at afhjælpe den uigennemsigtighed, der kan gøre visse AI-systemer uforståelige eller for komplekse for fysiske personer, bør der kræves en vis grad af gennemsigtighed for højrisiko-AI-systemer. Brugere bør kunne fortolke systemets output og anvende det korrekt. Højrisiko-AI-systemer bør derfor ledsages af relevant dokumentation og en brugsanvisning og indeholde kortfattede og klare oplysninger, blandt andet om mulige risici med hensyn til grundlæggende rettigheder og forskelsbehandling, hvis det er relevant.
- (48) Højrisiko-AI-systemer bør udformes og udvikles på en sådan måde, at fysiske personer kan føre tilsyn med deres funktion. Udbyderen af systemet bør derfor fastlægge passende foranstaltninger til menneskeligt tilsyn, inden systemet bringes i omsætning eller tages i brug. Hvor det er relevant, bør sådanne foranstaltninger navnlig sikre, at systemet er underlagt den menneskelige operatør og indbyggede driftsmæssige begrænsninger, som ikke kan tilsidesættes af systemet selv, og at de fysiske personer, som fører det menneskelige tilsyn, har de nødvendige kompetencer og den nødvendige uddannelse og beføjelse til at varetage rollen.
- (49) Højrisiko-AI-systemer bør fungere konsekvent i hele deres livscyklus og have et passende niveau af nøjagtighed, robusthed og cybersikkerhed i overensstemmelse med det generelt anerkendte aktuelle teknologiske niveau. Niveauet og parametrene med hensyn til nøjagtighed bør formidles til brugerne.

- (50) Den tekniske robusthed er et centralt krav for højrisiko-AI-systemer. De bør være modstandsdygtige over for risici, der er forbundet med systemets begrænsninger (f.eks. fejl, svigt, uoverensstemmelser og uventede situationer) og mod ondsindede handlinger, der kan bringe AI-systemets sikkerhed i fare og resultere i skadelig eller på anden vis uønsket adfærd. Manglende beskyttelse mod disse risici kan have sikkerhedsmæssige konsekvenser eller en negativ indvirkning på de grundlæggende rettigheder, f.eks. som følge af fejlagtige beslutninger eller forkerte eller partiske output, der er genereret af AI-systemet.
- (51) Cybersikkerhed spiller en afgørende rolle med hensyn til at sikre, at AI-systemer er modstandsdygtige over for forsøg på at ændre deres anvendelse, adfærd, ydeevne eller kompromittere deres sikkerhedsegenskaber fra ondsindede tredjeparter, der udnytter systemets sårbarheder. Cyberangreb mod AI-systemer kan udnytte AI-specifikke aktiver såsom træningsdatasæt (f.eks. dataforgiftning) eller trænedede modeller (f.eks. fjendtlige angreb) eller udnytte sårbarheder i AI-systemets digitale aktiver eller den underliggende IKT-infrastruktur. For at sikre et cybersikkerhedsniveau, der er passende i forhold til risiciene, bør udbydere af højrisiko-AI-systemer træffe passende foranstaltninger, idet der også tages hensyn til den underliggende IKT-infrastruktur, hvis det er relevant.
- (52) Som led i Unionens harmoniseringslovgivning bør der fastsættes regler for omsætning, ibrugtagning og anvendelse af højrisiko-AI-systemer i overensstemmelse med Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 om kravene til akkreditering og markedsovervågning af produkter<sup>51</sup>, Europa-Parlamentets og Rådets afgørelse nr. 768/2008/EF om fælles rammer for markedsføring af produkter<sup>52</sup> og Europa-Parlamentets og Rådets forordning (EU) 2019/1020 om markedsovervågning og produktoverensstemmelse<sup>53</sup> ("den nye lovgivningsmæssige ramme for markedsføring af produkter").
- (53) En bestemt fysisk eller juridisk person, defineret som udbyderen, bør påtage sig ansvaret for at omsætte eller ibrugtage et højrisiko-AI-system, uanset om denne fysiske eller juridiske person er den person, der har udformet eller udviklet systemet.
- (54) Udbyderen bør etablere et fornuftigt kvalitetsstyringssystem, sikre gennemførelsen af den påkrævede overensstemmelsesvurderingsprocedure, udarbejde den relevante dokumentation og indføre et robust system til overvågning efter omsætningen. Offentlige myndigheder, der ibrugtager højrisiko-AI-systemer til eget brug, kan vedtage og gennemføre reglerne for kvalitetsstyringssystemet som en del af det kvalitetsstyringssystem, der er vedtaget på nationalt eller regionalt plan, alt efter hvad der er relevant, under hensyntagen til de særlige forhold i sektoren og den pågældende offentlige myndigheds kompetencer og organisation.
- (55) Hvis et højrisiko-AI-system, som er en sikkerhedskomponent i et produkt, der er omfattet af relevant lovgivning inden for den nye lovgivningsmæssige ramme, ikke

---

<sup>51</sup> Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 af 9. juli 2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter og om ophævelse af Rådets forordning (EØF) nr. 339/93 (EUT L 218 af 13.8.2008, s. 30).

<sup>52</sup> Europa-Parlamentets og Rådets afgørelse nr. 768/2008/EF af 9. juli 2008 om fælles rammer for markedsføring af produkter og om ophævelse af Rådets afgørelse 93/465/EØF (EUT L 218 af 13.8.2008, s. 82).

<sup>53</sup> Europa-Parlamentets og Rådets forordning (EU) 2019/1020 af 20. juni 2019 om markedsovervågning og produktoverensstemmelse og om ændring af direktiv 2004/42/EF og forordning (EF) nr. 765/2008 og (EU) nr. 305/2011 (EUT L 169 af 25.6.2019, s. 1).

bringes i omsætning eller tages i brug uafhængigt af produktet, bør producenten af slutproduktet som defineret i lovgivningen inden for den nye lovgivningsmæssige ramme opfylde de forpligtelser, der påhviler udbyderen i henhold til denne forordning, og navnlig sikre, at det AI-system, der er indlejret i slutproduktet, opfylder kravene i denne forordning.

- (56) For at muliggøre håndhævelsen af denne forordning og skabe lige vilkår for operatørerne og under hensyntagen til de forskellige former for tilgængeliggørelse af digitale produkter er det vigtigt at sikre, at en person, der er etableret i Unionen, under alle omstændigheder kan give myndighederne alle de nødvendige oplysninger om et AI-systems overensstemmelse med reglerne. Hvis der ikke kan udpeges en importør, skal udbydere, der er etableret uden for Unionen, inden deres AI-systemer gøres tilgængelige i Unionen, derfor ved skriftlig fuldmagt udpege en bemyndiget repræsentant, der er etableret i Unionen.
- (57) I overensstemmelse med principperne i den nye lovgivningsmæssige ramme bør der fastsættes specifikke forpligtelser for de relevante økonomiske operatører såsom importører og distributører for at sikre retssikkerhed og lette disse aktørers overholdelse af lovgivningen.
- (58) I betragtning af AI-systemers karakter og de risici for sikkerheden og de grundlæggende rettigheder, der kan være forbundet med deres anvendelse, herunder behovet for at sikre korrekt overvågning af et AI-systems ydeevne i virkelige rammer, bør der fastsættes specifikke ansvarsområder for brugere. Brugere bør navnlig anvende højrisiko-AI-systemer i overensstemmelse med brugsanvisningen, og der bør fastsættes visse andre forpligtelser med hensyn til overvågning af AI-systemernes funktion og, hvor det er relevant, med hensyn til registrering.
- (59) Det bør fastsættes, at brugeren af AI-systemet skal være den fysiske eller juridiske person, offentlige myndighed, det agentur eller et andet organ, under hvis myndighed AI-systemet drives, undtagen hvis anvendelsen sker som led i en personlig ikkeerhvervsmæssig aktivitet.
- (60) I betragtning af kompleksiteten af værdikæden for kunstig intelligens bør relevante tredjeparter, navnlig de, der er involveret i salg og levering af software, softwareværktøjer og -komponenter, forhåndstrænede modeller og data, eller udbydere af netværkstjenester, samarbejde med udbydere og brugere i det omfang, det er relevant, for at gøre det muligt for dem at opfylde forpligtelserne i henhold til denne forordning og med de kompetente myndigheder, der er fastlagt i henhold til denne forordning.
- (61) Standardisering bør spille en central rolle med hensyn til at levere tekniske løsninger til udbyderne for at sikre overholdelsen af denne forordning. Overholdelse af harmoniserede standarder som defineret i Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012<sup>54</sup> bør være et middel for udbydere til at påvise overensstemmelse med kravene i denne forordning. Kommissionen kan imidlertid vedtage fælles tekniske specifikationer på områder, hvor der ikke findes harmoniserede standarder, eller hvor de er utilstrækkelige.

---

<sup>54</sup> Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF (EUT L 316 af 14.11.2012, s. 12).

- (62) For at sikre en høj grad af pålidelighed i højrisiko-AI-systemer bør disse systemer underkastes en overensstemmelsesvurdering, inden de bringes i omsætning eller tages i brug.
- (63) For så vidt angår højrisiko-AI-systemer, der vedrører produkter, der er omfattet af eksisterende EU-harmoniseringslovgivning som følge af tilgangen med den nye lovgivningsmæssige ramme, bør disse AI-systemers overensstemmelse med kravene i denne forordning vurderes som led i den overensstemmelsesvurdering, der allerede er fastsat i nævnte lovgivning, således at byrden for operatørerne minimeres, og enhver mulig overlappning undgås. Anvendeligheden af kravene i denne forordning bør derfor ikke påvirke den specifikke logik, metode eller generelle struktur for overensstemmelsesvurderingen i henhold til den relevante specifikke lovgivning inden for den nye lovgivningsmæssige ramme. Denne tilgang afspejles fuldt ud i samspillet mellem denne forordning og [maskinforordningen]. Selv om sikkerhedsrisici ved de AI-systemer, der sørger for sikkerhedsfunktioner i maskiner, er omfattet af kravene i denne forordning, vil visse specifikke krav i [maskinforordningen] sikre, at AI-systemet integreres i den samlede maskine på sikker vis, således at sikkerheden for maskinen som helhed ikke bringes i fare. I [maskinforordningen] anvendes samme definition af et AI-system som i denne forordning.
- (64) I betragtning af den mere omfattende erfaring, som professionelle, der udfører certificering forud for omsætning, har inden for produktsikkerhed og de relevante risici forskellige karakter, bør anvendelsesområdet for af tredjepart foretagne overensstemmelsesvurderinger af andre højrisiko-AI-systemer end dem, der vedrører produkter, begrænses i det mindste i den indledende fase af anvendelsen af denne forordning. Overensstemmelsesvurderinger af sådanne systemer bør derfor som hovedregel foretages af udbyderen på dennes eget ansvar, med undtagelse af AI-systemer, der er beregnet til at blive anvendt til biometrisk fjernidentifikation af personer, for hvilke det bør være muligt at inddrage et bemyndiget organ i overensstemmelsesvurderingen, i det omfang de ikke er forbudt.
- (65) Med henblik på af tredjeparter foretagne overensstemmelsesvurderinger af AI-systemer, der er beregnet til at blive anvendt til biometrisk fjernidentifikation af personer, bør der udpeges bemyndigede organer i henhold til denne forordning af de nationale kompetente myndigheder, forudsat at de opfylder en række krav, navnlig med hensyn til uafhængighed, kompetencer og interessekonflikter.
- (66) I overensstemmelse med det almindeligt anerkendte begreb væsentlig ændring for produkter, der er reguleret af EU-harmoniseringslovgivningen, bør et AI-system underkastes en ny overensstemmelsesvurdering, når der sker en ændring, som kan have indflydelse på systemets overensstemmelse med denne forordning, eller når systemets tilsigtede formål ændrer sig. Med hensyn til AI-systemer, der fortsætter med at "lære" efter, at de er bragt i omsætning eller taget i brug (dvs. de automatisk tilpasser, hvordan funktionerne udføres), er det desuden nødvendigt at fastsætte regler for, at ændringer af algoritmen og dens ydeevne, som er fastlagt på forhånd af udbyderen og vurderet på tidspunktet for overensstemmelsesvurderingen, ikke bør udgøre en væsentlig ændring.
- (67) Højrisiko-AI-systemer bør være forsynet med CE-mærkning for at vise, at de er i overensstemmelse med denne forordning, således at de kan bevæge sig frit på det indre marked. Medlemsstaterne bør ikke skabe uberettigede hindringer for omsætningen eller ibrugtagningen af højrisiko-AI-systemer, der opfylder kravene i denne forordning, og som er forsynet med CE-mærkning.

- (68) Under visse omstændigheder kan hurtig adgang til innovative teknologier være afgørende for menneskers sundhed og sikkerhed og for samfundet som helhed. Medlemsstaterne bør derfor af ekstraordinære hensyn til den offentlige sikkerhed eller beskyttelsen af fysiske personers liv og sundhed og beskyttelsen af industriel og kommerciel ejendomsret kunne tillade omsætning eller ibrugtagning af AI-systemer, der ikke har været genstand for en overensstemmelsesvurdering.
- (69) For at lette Kommissionens og medlemsstaternes arbejde inden for kunstig intelligens og øge gennemsigtigheden for offentligheden bør udbydere af andre højrisiko-AI-systemer end dem, der vedrører produkter, der er omfattet af relevant eksisterende EU-harmoniseringslovgivning, pålægges at registrere deres højrisiko-AI-system i en EU-database, der skal oprettes og forvaltes af Kommissionen. Kommissionen bør være dataansvarlig for denne database i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2018/1725<sup>55</sup>. For at sikre at databasen fungerer efter hensigten, når den tages i brug, bør proceduren for oprettelse af databasen omfatte, at Kommissionen udarbejder funktions-specifikationer, samt en uafhængig revisionsrapport.
- (70) Visse AI-systemer, der er beregnet til at interagere med fysiske personer eller generere indhold, kan indebære særlige risici for imitation eller vildledning, uanset om de er klassificeret som højrisikosystemer eller ej. Under visse omstændigheder bør anvendelsen af disse systemer derfor være underlagt særlige gennemsigtighedsforpligtelser, uden at dette berører kravene og forpligtelserne for højrisiko-AI-systemer. Fysiske personer bør navnlig underrettes om, at de interagerer med et AI-system, medmindre dette fremgår tydeligt af omstændighederne og konteksten for anvendelsen. Fysiske personer bør desuden underrettes, når de udsættes for et system til følelsesgenkendelse eller et system til biometrisk kategorisering. Sådanne oplysninger og underretninger bør gives i formater, der er tilgængelige for personer med handicap. Endvidere bør de brugere, der anvender et AI-system til at generere eller manipulere billed-, lyd- eller videoindhold, der i væsentlig grad ligner faktiske personer, steder eller begivenheder, og som fejlagtigt vil fremstå ægte, oplyse, at indholdet er kunstigt skabt eller manipuleret, ved at mærke outputtet og oplyse om dets kunstige oprindelse.
- (71) Kunstig intelligens er en hurtigt voksende vifte af teknologier, der kræver nye former for myndighedstilsyn og et sikkert område til forsøg, samtidig med at der sikres ansvarlig innovation og integration af passende sikkerhedsforanstaltninger og risikobegrænsende foranstaltninger. For at sikre en lovgivningsmæssig ramme, der er innovationsvenlig, fremtidssikret og modstandsdygtig over for forstyrrelser, bør de nationale kompetente myndigheder i en eller flere medlemsstater tilskyndes til at oprette reguleringsmæssige sandkasser for kunstig intelligens for at lette udviklingen og prøvningen af innovative AI-systemer under strengt myndighedstilsyn, før disse systemer bringes i omsætning eller på anden måde tages i brug.
- (72) Formålet med de reguleringsmæssige sandkasser bør være at fremme innovation inden for kunstig intelligens ved at skabe et kontrolleret forsøgs- og prøvningsmiljø i udviklingsfasen forud for omsætning med henblik på at sikre, at de innovative AI-

---

<sup>55</sup> Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

systemer er i overensstemmelse med denne forordning og anden relevant EU-lovgivning og national lovgivning, og øge retssikkerheden for innovatorer og de kompetente myndigheders tilsyn og forståelse af de muligheder, nye risici og virkninger, der er forbundet med anvendelsen af kunstig intelligens, samt fremskynde adgangen til markeder, herunder ved at fjerne hindringer for små og mellemstore virksomheder (SMV'er) og startup-virksomheder. For at sikre en ensartet gennemførelse i hele Unionen samt stordriftsfordele bør der fastsættes fælles regler for gennemførelsen af de reguleringsmæssige sandkasser og en ramme for samarbejde mellem de relevante myndigheder, der er involveret i tilsynet med sandkasserne. Denne forordning bør udgøre retsgrundlaget for anvendelsen af personoplysninger, der er indsamlet til andre formål med henblik på udvikling af visse AI-systemer i almenhedens interesse inden for rammerne af den reguleringsmæssige sandkasse for kunstig intelligens, jf. artikel 6, stk. 4, i forordning (EU) 2016/679 og artikel 6 i forordning (EU) 2018/1725 for så vidt andet ikke er fastsat i artikel 4, stk. 2, i direktiv (EU) 2016/680. Deltagerne i sandkassen bør sørge for passende sikkerhedsforanstaltninger og samarbejde med de kompetente myndigheder, herunder ved at følge deres vejledning og handle hurtigt og i god tro for at afbøde eventuelle store risici med hensyn til sikkerhed og de grundlæggende rettigheder, som måtte opstå under udviklingen og forsøgene i sandkassen. Der bør tages hensyn til adfærden hos deltagerne i sandkassen, når de kompetente myndigheder træffer afgørelse om pålæggelse af en administrativ bøde, jf. artikel 83, stk. 2, i forordning (EU) 2016/679 og artikel 57 i direktiv (EU) 2016/680.

- (73) For at fremme og beskytte innovationen er det vigtigt, at der tages særligt hensyn til mindre udbydere og brugere af AI-systemers interesser. Med henblik herpå bør medlemsstaterne udarbejde initiativer, der er rettet mod disse operatører, som f.eks. oplysningskampagner, information og kommunikation. Desuden skal der tages hensyn til mindre udbydere særlige interesser og behov, når bemyndigede organer fastsætter gebyrer for overensstemmelsesvurderinger. Udgifter forbundet oversættelse af påkrævet dokumentation og kommunikation med myndigheder kan udgøre en betydelig omkostning for udbydere og andre operatører, navnlig mindre udbydere og operatører. Medlemsstaterne bør muligvis sørge for, at et af de sprog, som de bestemmer sig for og accepterer med hensyn til de relevante udbydere dokumentation og kommunikationen med operatører, er et sprog, der forstås bredt af det størst mulige antal brugere på tværs af grænserne.
- (74) For at minimere risiciene i gennemførelsen som følge af manglende viden og ekspertise på markedet samt for at gøre det lettere for udbydere og bemyndigede organer at overholde deres forpligtelser i henhold til denne forordning bør AI-on-demand-plattformen, de europæiske digitale innovationsknudepunkter og de prøvnings- og forsøgsfaciliteter, som Kommissionen og medlemsstaterne har oprettet på nationalt plan eller EU-plan, eventuelt bidrage til gennemførelsen af denne forordning. Inden for rammerne af deres respektive opgave- og kompetenceområde kan de navnlig yde teknisk og videnskabelig støtte til udbydere og bemyndigede organer.
- (75) Kommissionen bør så vidt muligt lette adgangen til prøvnings- og forsøgsfaciliteter for organer, grupper eller laboratorier, der er oprettet eller akkrediteret i henhold til relevant EU-harmoniseringslovgivning, og som udfører opgaver i forbindelse med overensstemmelsesvurderinger af produkter eller udstyr, der er omfattet af EU-harmoniseringslovgivningen. Dette er navnlig tilfældet for ekspertpaneler, ekspertlaboratorier og referencelaboratorier på området for medicinsk udstyr, jf. forordning (EU) 2017/745 og forordning (EU) 2017/746.

- (76) For at fremme en gnidningsløs, effektiv og harmoniseret gennemførelse af denne forordning bør der nedsættes et europæisk udvalg for kunstig intelligens. Udvalget bør være ansvarligt for en række rådgivningsopgaver såsom udtalelser, henstillinger, rådgivning eller vejledning om spørgsmål vedrørende gennemførelsen af denne forordning, herunder med hensyn til tekniske specifikationer eller eksisterende standarder, der er relateret til de krav, der er fastsat i denne forordning, samt rådgive og bistå Kommissionen i forbindelse med specifikke spørgsmål vedrørende kunstig intelligens.
- (77) Medlemsstaterne spiller en central rolle i anvendelsen og håndhævelsen af denne forordning. I den forbindelse bør hver medlemsstat udpege en eller flere nationale kompetente myndigheder til at føre tilsyn med anvendelsen og gennemførelsen af denne forordning. For at øge organisationseffektiviteten for medlemsstaternes vedkommende og for at oprette et officielt kontaktpunkt for offentligheden og andre modparter på nationalt plan og EU-plan bør der i hver medlemsstat udpeges en national myndighed som national tilsynsmyndighed.
- (78) Alle udbydere bør have et system til overvågning efter omsætning, således at det sikres, at udbydere af højrisiko-AI-systemer tager erfaringerne med anvendelse af højrisiko-AI-systemer i betragtning, når de vil forbedre deres systemer og design- og udviklingsprocessen, og at de kan træffe eventuelle korrigerende foranstaltninger rettidigt. Dette system er også afgørende for at sikre, at eventuelle risici som følge af AI-systemer, der fortsætter med at "lære" efter at være bragt i omsætning eller taget i brug, kan imødegås mere effektivt og rettidigt. I den forbindelse bør udbyderne også forpligtes til at have et system til indberetning til de relevante myndigheder af alvorlige hændelser eller overtrædelser af national lovgivning eller EU-lovgivning, der beskytter de grundlæggende rettigheder som følge af anvendelsen af deres AI-systemer.
- (79) For at sikre en hensigtsmæssig og effektiv håndhævelse af de krav og forpligtelser, der er fastsat i denne forordning, som udgør EU-harmoniseringslovgivning, bør det system til markedsovervågning og produktoverensstemmelse, der er indført ved forordning (EU) 2019/1020, finde anvendelse i sin helhed. Nationale offentlige myndigheder eller organer, der fører tilsyn med anvendelsen af EU-lovgivningen om beskyttelse af grundlæggende rettigheder, herunder ligestillingsorganer, bør i det omfang, det er nødvendigt for deres mandat, også have adgang til al den dokumentation, der er udarbejdet i henhold til denne forordning.
- (80) EU-lovgivningen om finansielle tjenesteydelser omfatter regler og krav vedrørende intern forvaltning og risikostyring, som finder anvendelse på regulerede finansielle institutioner i forbindelse med leveringen af sådanne tjenester, også når de gør brug af AI-systemer. For at sikre en sammenhængende anvendelse og håndhævelse af forpligtelserne i henhold til denne forordning og de relevante regler og krav i EU-lovgivningen om finansielle tjenesteydelser bør de myndigheder, der er ansvarlige for tilsyn med og håndhævelse af lovgivningen om finansielle tjenesteydelser, herunder Den Europæiske Centralbank, i det omfang, det er relevant, udpeges som kompetente myndigheder med henblik på at føre tilsyn med gennemførelsen af denne forordning, herunder også markedsovervågningsaktiviteter, for så vidt angår AI-systemer, der leveres eller anvendes af finansielle institutioner, som er regulerede, og som der føres tilsyn med. For yderligere at styrke sammenhængen mellem denne forordning og de regler, der gælder for kreditinstitutter, der er reguleret ved Europa-Parlamentets og

Rådets direktiv 2013/36/EU<sup>56</sup>, bør overensstemmelsesvurderingsproceduren og nogle af udbydernes proceduremæssige forpligtelser i forbindelse med risikostyring, overvågning efter omsætning og dokumentation indarbejdes i de eksisterende forpligtelser og procedurer i henhold i direktiv 2013/36/EU. For at undgå overlappninger bør der også overvejes begrænsede undtagelser for så vidt angår udbydernes kvalitetsstyringssystem og den overvågningsforpligtelse, der pålægges brugere af højrisiko-AI-systemer, i det omfang disse gælder for kreditinstitutter, der er reguleret ved direktiv 2013/36/EU.

- (81) Udviklingen af andre AI-systemer end højrisiko-AI-systemer i overensstemmelse med kravene i denne forordning kan føre til en større udbredelse af pålidelig kunstig intelligens i Unionen. Udbydere af AI-systemer, der ikke er højrisikosystemer, bør tilskyndes til at udarbejde adfærdskodekser med det formål at fremme frivillig anvendelse af de obligatoriske krav, der gælder for højrisiko-AI-systemer. Udbydere bør også tilskyndes til på frivillig basis at anvende yderligere krav vedrørende f.eks. miljømæssig bæredygtighed, tilgængelighed for personer med handicap, interessenters deltagelse i udformningen og udviklingen af AI-systemer og mangfoldigheden i udviklingsteamene. For at fremme mindskelsen af tekniske hindringer for grænseoverskridende udveksling af data til udvikling af kunstig intelligens kan Kommissionen udvikle initiativer, blandt andet på sektorniveau, vedrørende f.eks. dataadgangsinfrastruktur og semantisk og teknisk interoperabilitet for forskellige typer data.
- (82) Det er vigtigt, at AI-systemer vedrørende produkter, der ikke er højrisikoprodukter i henhold til denne forordning og derfor ikke skal opfylde kravene heri, ikke desto mindre er sikre, når de bringes i omsætning eller tages i brug. Med henblik på at bidrage til dette mål vil Europa-Parlamentets og Rådets direktiv 2001/95/EF<sup>57</sup> finde anvendelse som et sikkerhedsnet.
- (83) For at sikre et tillidsfuldt og konstruktivt samarbejde mellem de kompetente myndigheder på EU-plan og nationalt plan bør alle de parter, der er involveret i anvendelsen af denne forordning, respektere fortroligheden af oplysninger og data, der er indhentet under udførelsen af deres opgaver.
- (84) Medlemsstaterne bør træffe alle nødvendige foranstaltninger til at sikre, at bestemmelserne i denne forordning gennemføres, herunder ved at fastsætte sanktioner for overtrædelse heraf, som er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning. Med hensyn til visse specifikke overtrædelser bør medlemsstaterne tage hensyn til de margener og kriterier, der er fastsat i denne forordning. Den Europæiske Tilsynsførende for Databeskyttelse bør have beføjelse til at pålægge de af Unionens institutioner, agenturer og organer, der er omfattet af denne forordnings anvendelsesområde, bøder.
- (85) For at den lovgivningsmæssige ramme om nødvendigt kan tilpasses, bør Kommissionen delegeres beføjelse til at vedtage retsakter, jf. artikel 290 i TEUF, med henblik på at ændre de i bilag I omhandlede teknikker og tilgange til at definere AI-

---

<sup>56</sup> Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF (EUT L 176 af 27.6.2013, s. 338).

<sup>57</sup> Europa-Parlamentets og Rådets direktiv 2001/95/EF af 3. december 2001 om produktsikkerhed i almindelighed (EFT L 11 af 15.1.2002, s. 4).



systemer, den i bilag II anførte EU-harmoniseringslovgivning, de i bilag III anførte højrisiko-AI-systemer, de i bilag IV anførte bestemmelser vedrørende teknisk dokumentation, indholdet af EU-overensstemmelseserklæringen i bilag V, bestemmelserne vedrørende overensstemmelsesvurderingsprocedurer i bilag VI og VII og bestemmelserne om fastsættelse af de højrisiko-AI-systemer, på hvilke overensstemmelsesvurderingsproceduren på grundlag af en vurdering af kvalitetsstyringssystemet og en vurdering af den tekniske dokumentation skal finde anvendelse. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning<sup>58</sup>. For at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet navnlig alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i de af Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.

- (86) For at sikre ensartede betingelser for gennemførelsen af denne forordning bør Kommissionen tillægges gennemførelsesbeføjelser. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011<sup>59</sup>.
- (87) Målet for denne forordning kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af handlingens omfang og virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i TEU. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke videre, end hvad der er nødvendigt for at nå dette mål.
- (88) Denne forordning bør anvendes fra den [Publikationskontoret — *indsæt datoen i artikel 85*]. Infrastrukturen i forbindelse med forvaltnings- og overensstemmelsesvurderingssystemet bør dog være operationel inden denne dato, og bestemmelserne om bemyndigede organer og forvaltningsstruktur bør derfor finde anvendelse fra den [*Publikationskontoret — indsæt dato: tre måneder efter denne forordnings ikrafttræden*]. Desuden bør medlemsstaterne fastsætte og meddele Kommissionen bestemmelser om sanktioner, herunder administrative bøder, og sikre, at de er gennemført korrekt og effektivt på datoen for denne forordnings anvendelse. Bestemmelserne om sanktioner bør derfor finde anvendelse fra den [*Publikationskontoret — indsæt dato: tolv måneder efter denne forordnings ikrafttræden*].
- (89) Den Europæiske Tilsynsførende for Databeskyttelse og Det Europæiske Databeskyttelsesråd er blevet hørt i overensstemmelse med artikel 42, stk. 2, i forordning (EU) 2018/1725 og afgav en udtalelse den [...].

---

<sup>58</sup> EUT L 123 af 12.5.2016, s. 1.

<sup>59</sup> Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13).

VEDTAGET DENNE FORORDNING:

## AFSNIT I

### ALMINDELIGE BESTEMMELSER

#### *Artikel 1 Genstand*

Ved denne forordning fastsættes:

- (a) harmoniserede regler for omsætning, ibrugtagning og anvendelse af systemer med kunstig intelligens ("AI-systemer") i Unionen
- (a) forbud mod visse former for praksis med hensyn til kunstig intelligens
- (b) specifikke krav til højrisiko-AI-systemer og forpligtelser for operatører af sådanne systemer
- (c) harmoniserede gennemsigtighedsregler for AI-systemer, der er beregnet til at interagere med fysiske personer, systemer til følelsesgenkendelse og systemer til biometriske kategorisering, samt AI-systemer, der anvendes til at generere eller manipulere billed-, lyd- eller videoindhold
- (d) regler om markedsovervågning og -tilsyn.

#### *Artikel 2 Anvendelsesområde*

1. Denne forordning finder anvendelse på:
  - (a) udbydere, der omsætter eller ibrugtager AI-systemer i Unionen, uanset om samme udbydere er etablerede i Unionen eller i et tredjeland
  - (b) brugere af AI-systemer i Unionen
  - (c) udbydere og brugere af AI-systemer, der befinder sig i et tredjeland, hvis det output, der produceres af systemet, anvendes i Unionen.
2. For så vidt angår højrisiko-AI-systemer, der er sikkerhedskomponenter i produkter eller systemer, eller som selv er produkter eller systemer, der er omfattet af anvendelsesområdet for følgende retsakter, finder kun artikel 84 i denne forordning anvendelse:
  - (a) forordning (EF) nr. 300/2008
  - (b) forordning (EU) nr. 167/2013
  - (c) forordning (EU) nr. 168/2013
  - (d) direktiv 2014/90/EU
  - (e) direktiv (EU) 2016/797
  - (f) forordning (EU) 2018/858
  - (g) forordning (EU) 2018/1139
  - (h) forordning (EU) 2019/2144.

3. Denne forordning finder ikke anvendelse på AI-systemer, der er udviklet eller udelukkende anvendes til militære formål.
4. Denne forordning finder ikke anvendelse på offentlige myndigheder i tredjelande eller internationale organisationer, der er omfattet af denne forordnings anvendelsesområde, jf. stk. 1, hvis disse myndigheder eller organisationer anvender AI-systemer inden for rammerne af internationale aftaler om retshåndhævelse og retligt samarbejde med Unionen eller med en eller flere medlemsstater.
5. Denne forordning berører ikke anvendelsen af bestemmelserne om formidleransvar for tjenesteydere i kapitel II, afdeling IV, i Europa-Parlamentets og Rådets direktiv 2000/31/EF<sup>60</sup> [*skal erstattes af de tilsvarende bestemmelser i retsakten om digitale tjenester*].

### *Artikel 3* *Definitioner*

I denne forordning forstås ved:

- (1) "system med kunstig intelligens" (AI-system): software, der er udviklet ved hjælp af en eller flere af de i bilag I anførte teknikker og tilgange, og som med henblik på et givet sæt mål, der er fastsat af mennesker, kan generere output såsom indhold, forudsigelser, anbefalinger eller beslutninger, der påvirker de miljøer, de interagerer med
- (2) "udbyder": en fysisk eller juridisk person, en offentlig myndighed, et agentur eller et andet organ, der udvikler eller får udviklet et AI-system med henblik på at bringe det i omsætning eller ibrugtage det under eget navn eller varemærke, enten mod betaling eller gratis
- (3) "mindre udbyder": en udbyder, der er en mikrovirksomhed eller en mindre virksomhed som defineret i Kommissionens henstilling 2003/361/EF<sup>61</sup>
- (4) "bruger": enhver fysisk eller juridisk person, offentlig myndighed eller ethvert agentur eller andet organ, der anvender et AI-system under sin myndighed, medmindre AI-systemet anvendes som led i en personlig ikkeerhvervsmæssig aktivitet
- (5) "bemyndiget repræsentant": enhver fysisk eller juridisk person, der er etableret i Unionen, og som har modtaget en skriftlig fuldmagt fra en udbyder af et AI-system til på dennes vegne at opfylde og udføre de forpligtelser og procedurer, der er fastsat i denne forordning
- (6) "importør": enhver fysisk eller juridisk person, der er etableret i Unionen, og som omsætter eller ibrugtager et AI-system, der bærer en uden for Unionen etableret fysisk eller juridisk persons navn eller varemærke
- (7) "distributør": enhver fysisk eller juridisk person i forsyningskæden ud over udbyderen eller importøren, som gør et AI-system tilgængeligt på EU-markedet uden at have indflydelse på dets egenskaber

---

<sup>60</sup> Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked ("Direktivet om elektronisk handel") (EFT L 178 af 17.7.2000, s. 1).

<sup>61</sup> Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (EUT L 124 af 20.5.2003, s. 36).

- (8) "operatør": udbyderen, brugeren, den bemyndigede repræsentant, importøren og distributøren
- (9) "bringe i omsætning": den første tilgængeliggørelse af et AI-system på EU-markedet
- (10) "tilgængeliggørelse på markedet": enhver levering af et AI-system med henblik på distribution eller anvendelse på EU-markedet som led i erhvervsvirksomhed mod eller uden vederlag
- (11) "ibrugtagning": levering af et AI-system med henblik på anvendelse for første gang enten direkte til brugeren eller til egen brug på EU-markedet i overensstemmelse med systemets tilsigtede formål
- (12) "tilsigtet formål": den anvendelse, som et AI-system af udbyderen er beregnet til, herunder den specifikke sammenhæng og de specifikke betingelser for anvendelse som angivet i de oplysninger, udbyderen har givet i brugsanvisningen, reklame- eller salgsmaterialet eller reklame- og salgserklæringerne samt i den tekniske dokumentation
- (13) "fejlanvendelse, der med rimelighed kan forudses": anvendelse af et AI-system på en måde, der ikke er i overensstemmelse med systemets tilsigtede formål, men som kan skyldes menneskelig adfærd eller interaktion med andre systemer, som med rimelighed kan forudses
- (14) "sikkerhedskomponent i et produkt eller et system": en komponent i et produkt eller et system, som har en sikkerhedsfunktion for det pågældende produkt eller system eller i tilfælde af svigt eller funktionsfejl, som bringer menneskers sundhed og sikkerhed eller ejendom i fare, i produktet eller systemet
- (15) "brugsanvisning": oplysninger fra udbyderen med henblik på at informere brugeren om navnlig et AI-systems tilsigtede formål og korrekte anvendelse, herunder de specifikke geografiske, adfærdsmæssige eller funktionelle rammer, inden for hvilke højrisiko-AI-systemet skal anvendes
- (16) "tilbagekaldelse af et AI-system": enhver foranstaltning, der har til formål at opnå, at et AI-system, der allerede er gjort tilgængeligt for brugerne, returneres til udbyderen
- (17) "tilbagetrækning af et AI-system": enhver foranstaltning, der har til formål at forhindre, at et AI-system distribueres, udstilles eller udbydes
- (18) "et AI-systems ydeevne": et AI-systems evne til at opfylde det tilsigtede formål
- (19) "bemyndigende myndighed": den nationale myndighed, der er ansvarlig for at indføre og gennemføre de nødvendige procedurer for vurdering, udpegelse og bemyndigelse af overensstemmelsesvurderingsorganer og for overvågning heraf
- (20) "overensstemmelsesvurdering": en proces til verificering af, om de i afsnit III, kapitel 2, i denne forordning fastsatte krav vedrørende et AI-system er opfyldt
- (21) "overensstemmelsesvurderingsorgan": et organ, der som tredjepart udfører overensstemmelsesvurderingsopgaver, herunder prøvning, certificering og inspektion
- (22) "bemyndiget organ": et overensstemmelsesvurderingsorgan, der er udpeget i overensstemmelse med denne forordning og anden relevant EU-harmoniseringslovgivning
- (23) "væsentlig ændring": en ændring af et AI-system efter dets omsætning eller ibrugtagning, som har indvirkning på AI-systemets overensstemmelse med de i

afsnit III, kapitel 2, i denne forordning fastsatte krav, eller som medfører en ændring af det tilsigtede formål, med hensyn til hvilket AI-systemet er vurderet

- (24) "CE-overensstemmelsesmærkning" (CE-mærkning): en mærkning, hvormed en udbyder angiver, at et AI-system er i overensstemmelse med de i afsnit III, kapitel 2, i denne forordning fastsatte krav og anden EU-lovgivning om harmonisering af betingelser for omsætning af produkter ("EU-harmoniseringslovgivning") og om anbringelse af denne mærkning
- (25) "overvågning efter omsætningen": alle aktiviteter, som udbydere af AI-systemer udfører for proaktivt at indhente og gennemgå erfaringer med anvendelse af de AI-systemer, de bringer i omsætning eller tager i brug, med henblik på at afdække eventuelle behov for straks at træffe nødvendige, korrigerende eller forebyggende foranstaltninger
- (26) "markedsovervågningsmyndighed": den nationale myndighed, der udfører aktiviteter og træffer foranstaltninger i henhold til forordning (EU) 2019/1020
- (27) "harmoniseret standard": en europæisk standard som defineret i artikel 2, nr. 1), litra c), i forordning (EU) nr. 1025/2012
- (28) "fælles specifikationer": et dokument, der ikke er en standard, og som indeholder tekniske løsninger, der giver mulighed for at opfylde visse krav og forpligtelser, der er fastsat i denne forordning
- (29) "træningsdata": data, der anvendes til træning af et AI-system ved hjælp af tilpasning af systemets lærbare parametre, herunder vægte i et neuralt netværk
- (30) "valideringsdata": data, der anvendes til at foretage en evaluering af det trænede AI-system og til at justere blandt andet systemets ikkelærbare parametre og dets læringsproces for at forhindre overtilpasning, idet valideringsdatasættet kan være et separat datasæt eller en del af træningsdatasættet med enten en fast eller en variabel opdeling
- (31) "prøvningsdata": data, der anvendes til en uafhængig evaluering af det trænede og validerede AI-system for at bekræfte systemets forventede ydeevne, inden det bringes i omsætning eller tages i brug
- (32) "inputdata": data, der leveres til eller hentes direkte af et AI-system, og på grundlag af hvilke systemet leverer et output
- (33) "biometriske data": personoplysninger, der som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende, som f.eks. ansigtsbilleder eller fingeraftryksoplysninger
- (34) "system til følelsesgenkendelse": et AI-system, der har til formål at genkende eller udlede fysiske personers følelser eller hensigter på grundlag af deres biometriske data
- (35) "system til biometrisk kategorisering": et AI-system, der har til formål at tildele fysiske personer bestemte kategorier såsom køn, alder, hårfarve, øjenfarve, tatoveringer, etnisk oprindelse, seksuel orientering eller politisk overbevisning på grundlag af deres biometriske data
- (36) "system til biometrisk fjernidentifikation": et AI-system, der har til formål at identificere fysiske personer på afstand ved at sammenligne en persons biometriske

data med de biometriske data i en referencedatabase, uden at brugeren af AI-systemet har forudgående viden om, hvorvidt personen vil være til stede og kan identificeres

- (37) "system til biometrisk fjernidentifikation i realtid": et system til biometrisk fjernidentifikation, hvor optagelse af biometriske data, sammenligning og identifikation finder sted uden væsentlig forsinkelse. Dette omfatter ikke blot øjeblikkelig identifikation, men også begrænsede, korte forsinkelser for at undgå omgåelse
- (38) "system til efterfølgende biometrisk fjernidentifikation": et system til biometrisk fjernidentifikation, som ikke er system til biometrisk fjernidentifikation i realtid
- (39) "offentlige steder": ethvert fysisk sted, der er tilgængeligt for offentligheden, uanset om visse betingelser for adgang finder anvendelse
- (40) "retshåndhævende myndigheder":
- (a) enhver offentlig myndighed, der er kompetent med hensyn til at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed, eller
  - (b) ethvert andet organ eller enhver anden enhed, som i henhold til medlemsstaternes nationale lovgivning udøver offentlig myndighed og offentlige beføjelser med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed
- (41) "retshåndhævelse": aktiviteter, som retshåndhævende myndigheder udfører med hensyn til at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed
- (42) "national tilsynsmyndighed": den myndighed, som en medlemsstat giver ansvaret for at gennemføre og anvende denne forordning, koordinere de aktiviteter, der er betroet den pågældende medlemsstat, fungere som eneste kontaktpunkt for Kommissionen og repræsentere medlemsstaten i Det Europæiske Udvalg for Kunstig Intelligens
- (43) "national kompetent myndighed": den nationale tilsynsmyndighed, den bemyndigende myndighed og markedsovervågningsmyndigheden
- (44) "alvorlig hændelse": enhver hændelse, som direkte eller indirekte fører, kunne have ført eller kan føre til et af følgende udfald:
- (a) et menneskes død eller alvorlig skade på et menneskes helbred eller ejendom eller på miljøet
  - (b) en alvorlig og uoprettelig forstyrrelse i forvaltningen og driften af kritisk infrastruktur.

#### *Artikel 4* *Ændring af bilag I*

Kommissionen tillægges beføjelse til at vedtage delegerede retsakter, jf. artikel 73, med henblik på at ændre listen over teknikker og tilgange i bilag I for at føre listen ajour med den markedsrelevante og tekniske udvikling på grundlag af egenskaber, der svarer til de oplyste teknikker og tilgange.

## AFSNIT II

### FORBUDT PRAKSIS MED HENSYN TIL KUNSTIG INTELLIGENS

#### *Artikel 5*

1. Følgende former for praksis med hensyn til kunstig intelligens er forbudt:
  - (a) omsætning, ibrugtagning eller anvendelse af et AI-system, der anvender subliminale teknikker, der rækker ud over den menneskelige bevidsthed, med henblik på i væsentlig grad at fordreje en persons adfærd på en måde, der påfører eller sandsynligvis vil påføre den pågældende person eller en anden person fysisk eller psykisk skade
  - (b) omsætning, ibrugtagning eller anvendelse af et AI-system, der udnytter enhver af en specifik gruppe af personers sårbarheder på grundlag af alder eller fysisk eller psykisk handicap med henblik på i væsentlig grad at fordreje en til gruppen hørende persons adfærd på en måde, der påfører eller sandsynligvis vil påføre den pågældende person eller en anden person fysisk eller psykisk skade
  - (c) omsætning, ibrugtagning eller anvendelse af AI-systemer fra offentlige myndigheders side eller på deres vegne med henblik på evaluering eller klassificering af fysiske personers troværdighed over en given periode på grundlag af deres sociale adfærd eller kendte eller forudsagte personlige egenskaber eller personlighedstræk, således at den sociale bedømmelse fører til et eller begge følgende udfald:
    - i) skadelig eller ugunstig behandling af visse fysiske personer eller hele grupper heraf i sociale sammenhænge, som ikke har noget at gøre med de sammenhænge, i hvilke dataene oprindeligt blev genereret eller indsamlet
    - ii) skadelig eller ugunstig behandling af visse fysiske personer eller hele grupper heraf, som er uberettiget eller uforholdsmæssig i forhold til deres sociale adfærd eller alvorligheden heraf
  - (d) anvendelse af systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse, medmindre og i det omfang en sådan anvendelse er strengt nødvendig for et af følgende formål:
    - i) målrettet eftersøgning af specifikke potentielle ofre for kriminalitet, herunder forsvundne børn
    - ii) forebyggelse af en specifik, væsentlig og overhængende trussel mod fysiske personers liv eller fysiske sikkerhed eller om et terrorangreb
    - iii) afsløring, lokalisering, identifikation eller retsforfølgning af en gerningsmand, der har begået, eller af en person, der mistænkes for at have begået, en strafbar handling, der er omhandlet i artikel 2, stk. 2, i Rådets rammeafgørelse 2002/584/JHA<sup>62</sup>, og som i den pågældende medlemsstat kan straffes med frihedsstraf eller en anden

---

<sup>62</sup> Rådets rammeafgørelse 2002/584/RIA af 13. juni 2002 om den europæiske arrestordre og om procedurerne for overgivelse mellem medlemsstaterne (EFT L 190 af 18.7.2002, s. 1).

frihedsberøvende foranstaltning af en maksimal varighed på mindst tre år som fastsat i denne medlemsstats lovgivning.

2. Ved anvendelse af systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse til et af de i stk. 1, litra d), omhandlede formål, tages der hensyn til følgende elementer:

- (a) karakteren af den situation, der giver anledning til den mulige anvendelse, navnlig alvorligheden, sandsynligheden og omfanget af den skade, der forvoldes, hvis systemet ikke anvendes
- (b) konsekvenserne for alle de berørte personers rettigheder og friheder, navnlig alvorligheden, sandsynligheden og omfanget af disse konsekvenser, hvis systemet anvendes.

Ved anvendelse af systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse til et af de i stk. 1, litra d), omhandlede formål overholdes desuden nødvendige og forholdsmæssige sikkerhedsforanstaltninger og betingelser vedrørende anvendelsen, navnlig for så vidt angår tidsmæssige, geografiske og personlige begrænsninger.

3. Hvad angår stk. 1, litra d), og stk. 2 er hver enkelt anvendelse af et system til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse betinget af en forudgående tilladelse, der er udstedt af en judiciel myndighed eller en uafhængig administrativ myndighed i den medlemsstat, hvor anvendelsen skal finde sted, på grundlag af en begrundet anmodning og i overensstemmelse med de detaljerede regler i national ret, jf. stk. 4. I behørigt begrundede hastetilfælde kan anvendelsen af systemet dog påbegyndes uden tilladelse, og der kan anmodes om tilladelse under eller efter anvendelsen.

Den kompetente judicielle eller administrative myndighed udsteder kun en tilladelse, hvis den på grundlag af objektive beviser eller klare indikationer, den får forelagt, finder det godtgjort, at anvendelsen af det pågældende system til biometrisk fjernidentifikation i realtid er nødvendig og rimelig for at opfylde et af de i stk. 1, litra d), anførte formål som påpeget i anmodningen. Når den kompetente judicielle eller administrative myndighed træffer afgørelse om anmodningen, tager den hensyn til de i stk. 2 omhandlede elementer.

4. En medlemsstat kan beslutte at give mulighed for helt eller delvist at tillade anvendelse af systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse inden for de begrænsninger og på de betingelser, der er nævnt i stk. 1, litra d), og stk. 2 og 3. Den pågældende medlemsstat fastsætter i sin nationale lovgivning de nødvendige detaljerede regler for anmodning, udstedelse og benyttelse af samt tilsyn i forbindelse med de i stk. 3 omhandlede tilladelser. Disse regler præciserer også, til hvilke af de i stk. 1, litra d), anførte formål, herunder for hvilke af de i nr. iii) nævnte strafbare handlinger, de kompetente myndigheder kan få tilladelse til at anvende disse systemer med henblik på retshåndhævelse.



## AFSNIT III

### HØJRISIKO-AI-SYSTEMER

#### KAPITEL 1

#### KLASSIFICERING AF AI-SYSTEMER SOM HØJRISIKOSYSTEMER

##### *Artikel 6*

##### *Klassificeringsregler for højrisiko-AI-systemer*

1. Uanset om et AI-system bringes i omsætning eller tages i brug uafhængigt af de i litra a) og b) omhandlede produkter, betragtes AI-systemet som et højrisikosystem, hvis begge følgende betingelser er opfyldt:
  - (a) AI-systemet er beregnet til at blive anvendt som en sikkerhedskomponent i et produkt eller er i sig selv et produkt, der er omfattet af den EU-harmoniseringslovgivning, der er anført i bilag II
  - (b) det produkt, hvis sikkerhedskomponent er AI-systemet, eller AI-systemet selv som et produkt skal underkastes en overensstemmelsesvurdering foretaget af tredjepart med henblik på omsætning eller ibrugtagning af produktet i henhold til den EU-harmoniseringslovgivning, der er anført i bilag II.
2. Ud over de højrisiko-AI-systemer, der er omhandlet i stk. 1, betragtes de AI-systemer, der er omhandlet i bilag III, også som højrisikosystemer.

##### *Artikel 7*

##### *Ændring af bilag III*

1. Kommissionen tillægges beføjelse til at vedtage delegerede retsakter, jf. artikel 73, med henblik på at ajourføre listen i bilag III ved at tilføje højrisiko-AI-systemer, hvis begge følgende betingelser er opfyldt:
  - (a) AI-systemerne er beregnet til at blive anvendt på et af de områder, der er anført i punkt 1-8 i bilag III
  - (b) AI-systemerne udgør en risiko for skade på menneskers sundhed og sikkerhed eller en risiko for negativ indvirkning på de grundlæggende rettigheder, som med hensyn til alvorlighed og sandsynlighed svarer til eller er større end risikoen for skade eller negativ indvirkning ved de højrisiko-AI-systemer, der allerede er nævnt i bilag III.
2. Ved vurdering, jf. stk. 1, af, om et AI-system udgør en risiko for skade på menneskers sundhed og sikkerhed eller en risiko for negativ indvirkning på de grundlæggende rettigheder, som svarer til eller er større end risikoen for skade ved de højrisiko-AI-systemer, der allerede er nævnt i bilag III, tager Kommissionen hensyn til følgende kriterier:
  - (a) det tilsigtede formål med AI-systemet
  - (b) i hvilket omfang AI-systemet er blevet anvendt eller sandsynligvis vil blive anvendt

- (c) i hvilket omfang anvendelsen af AI-systemet allerede har forvoldt skade på menneskers sundhed og sikkerhed, har haft negativ indvirkning på de grundlæggende rettigheder eller har givet anledning til betydelig bekymring med hensyn til forekomsten af en sådan skade eller negativ indvirkning, hvilket er afspejlet i rapporter eller dokumenterede påstande, der er indgivet til de nationale kompetente myndigheder
- (d) det potentielle omfang af en sådan skade eller negativ indvirkning, navnlig med hensyn til alvorlighed og mulighed for påvirkning af flere personer
- (e) i hvilket omfang potentielt skadede eller negativt påvirkede personer afhænger af det resultat, AI-systemet giver, navnlig hvis det af praktiske eller juridiske grunde ikke med rimelighed er muligt at fravælge resultatet
- (f) i hvilket omfang potentielt skadede eller negativt påvirkede personer befinder sig i en sårbar situation i forhold til brugeren af AI-systemet, navnlig som følge af en ubalance med hensyn til magt, viden, økonomiske eller sociale omstændigheder eller alder
- (g) i hvilket omfang det resultat, AI-systemet giver, let kan ændres, idet resultater, der har indvirkning på menneskers sundhed eller sikkerhed, ikke anses for let at kunne ændres
- (h) i hvilket omfang den eksisterende EU-lovgivning indeholder bestemmelser om:
  - i) effektive retsmidler med hensyn til de risici, der er forbundet med AI-systemer, med undtagelse af erstatningskrav
  - ii) effektive foranstaltninger til forebyggelse eller i væsentlig grad minimering af disse risici.

## KAPITEL 2

### KRAV TIL HØJRISIKO-AI-SYSTEMER

#### *Artikel 8* *Overholdelse af krav*

1. Højrisiko-AI-systemer opfylder de krav, der er fastsat i dette kapitel.
2. I sikringen af, at disse krav overholdes, tages højrisiko-AI-systemernes tilsigtede formål og det risikostyringssystem, der er omhandlet i artikel 9, i betragtning.

#### *Artikel 9* *Risikostyringssystem*

1. Hvad angår højrisiko-AI-systemer oprettes og gennemføres der et risikostyringssystem, som dokumenteres og vedligeholdes.
2. Risikostyringssystemet består af en kontinuerlig iterativ proces, der løber i hele højrisiko-AI-systemets livscyklus, og som kræver regelmæssig systematisk opdatering. Det omfatter følgende trin:
  - (a) kortlægning og analyse af kendte og forudsigelige risici forbundet med hvert højrisiko-AI-system

- (b) vurdering og evaluering af de risici, der kan opstå, når højrisiko-AI-systemet anvendes i overensstemmelse med dets tilsigtede formål og ved fejlanvendelse, der med rimelighed kan forudses
  - (c) evaluering af andre risici, der kan opstå, på grundlag af analyse af data indsamlet fra systemet til overvågning efter omsætningen, jf. artikel 61
  - (d) passende risikostyringsforanstaltninger i overensstemmelse med bestemmelserne i de følgende stykker.
3. De i stk. 2, litra d), omhandlede risikostyringsforanstaltninger tager behørigt hensyn til virkningerne af og eventuelle interaktioner som følge af den kombinerede anvendelse af kravene i kapitel 2. De tager hensyn til det generelt anerkendte aktuelle teknologiske niveau, herunder som afspejlet i relevante harmoniserede standarder eller fælles specifikationer.
4. De i stk. 2, litra d), omhandlede risikostyringsforanstaltninger er af en sådan art, at eventuelle resterende risici, der er forbundet med hver fare, samt den samlede resterende risiko ved højrisiko-AI-systemerne vurderes at være acceptabel, forudsat at højrisiko-AI-systemet anvendes i overensstemmelse med dets tilsigtede formål eller ved fejlanvendelse, der med rimelighed kan forudses. Disse resterende risici meddeles brugeren.

I fastlæggelsen af de mest hensigtsmæssige risikostyringsforanstaltninger sikres følgende:

- (a) fjernelse eller i videst mulig omfang begrænsning af risici ved hjælp af passende udformning og udvikling
- (b) om nødvendigt gennemførelse af passende foranstaltninger til afbødning og kontrol for så vidt angår risici, der ikke kan fjernes
- (c) tilvejebringelse af tilstrækkelige oplysninger, jf. artikel 13, navnlig for så vidt angår de risici, der er omhandlet i stk. 2, litra b), og, hvis det er relevant, uddannelse af brugerne.

Ved fjernelse eller begrænsning af risici, der er forbundet med anvendelsen af et højrisiko-AI-system, tages der behørigt hensyn til den tekniske viden, erfaring og uddannelse, som kan forventes af brugeren, og det miljø, i hvilket systemet er beregnet til at blive anvendt.

5. Højrisiko-AI-systemer prøves med henblik på at fastslå de mest hensigtsmæssige risikostyringsforanstaltninger. Prøvningen sikrer, at højrisiko-AI-systemer fungerer konsekvent i overensstemmelse med deres tilsigtede formål og opfylder de krav, der er fastsat i dette kapitel.
6. Prøvningsprocedurerne er egnede til at opfylde AI-systemets tilsigtede formål og behøver ikke gå videre, end hvad der er nødvendigt for at opfylde dette formål.
7. Prøvning af højrisiko-AI-systemer foretages på et hvilket som helst tidspunkt under hele udviklingsprocessen, alt efter hvad der er relevant, og under alle omstændigheder inden omsætning eller ibrugtagning. Prøvningen foretages på grundlag af på forhånd definerede parametre og sandsynlighedsbaserede tærskler, der står i et passende forhold til det tilsigtede formål med højrisiko-AI-systemet.
8. I gennemførelsen af det risikostyringssystem, der er beskrevet i stk. 1-7, tages der særligt hensyn til, om der er sandsynlighed for, at højrisiko-AI-systemet tilgås af eller har indvirkning på børn.

9. For kreditinstitutter, der er reguleret ved direktiv 2013/36/EU, er de aspekter, der er beskrevet i stk. 1-8, en del af de risikostyringsprocedurer, som institutterne har fastlagt i henhold til artikel 74 i nævnte direktiv.

*Artikel 10*  
*Data og datastyring*

1. De højrisiko-AI-systemer, der gør brug af teknikker, som omfatter træning af modeller med data, udvikles på grundlag af trænings-, validerings- og prøvningsdatasæt, der opfylder de kvalitetskriterier, der er omhandlet i stk. 2-5.
2. Trænings-, validerings- og prøvningsdatasæt er underlagt passende datastyrings- og dataforvaltningspraksisser. Disse praksisser vedrører navnlig:
  - (a) de relevante valg med hensyn til udformning
  - (b) dataindsamling
  - (c) relevant dataforberedelsesbehandling såsom annotation, mærkning, rensning, berigning og aggregering
  - (d) formuleringen af relevante antagelser, navnlig med hensyn til de oplysninger, som dataene skal måle og repræsentere
  - (e) en forudgående vurdering af tilgængeligheden, mængden og egnetheden af de datasæt, der er nødvendige
  - (f) undersøgelse med hensyn til mulig forudindtaget
  - (g) kortlægning af eventuelle datamangler eller datautilstrækkeligheder, og hvordan de kan afhjælpes.
3. Trænings-, validerings- og prøvningsdatasæt er relevante, repræsentative, fejlfri og fuldstændige. De har de tilstrækkelige statistiske egenskaber, herunder, hvis det er relevant, med hensyn til de personer eller grupper af personer, på hvilke højrisiko-AI-systemet skal anvendes. Disse egenskaber kan opfyldes for de enkelte datasæt eller for en kombination heraf.
4. I trænings-, validerings- og prøvningsdatasæt tages der i det omfang, det er nødvendigt i lyset af deres tilsigtede formål, hensyn til de egenskaber eller elementer, der er særlige for den specifikke geografiske, adfærdsmæssige eller funktionelle ramme, inden for hvilken højrisiko-AI-systemet skal anvendes.
5. I det omfang, det er strengt nødvendigt for at sikre, at forudindtaget i forbindelse med højrisiko-AI-systemer overvåges, opdages og korrigeres, kan udbydere af sådanne systemer behandle særlige kategorier af personoplysninger, der er omhandlet i artikel 9, stk. 1, i forordning (EU) 2016/679, artikel 10 i direktiv (EU) 2016/680 og artikel 10, stk. 1, i forordning (EU) 2018/1725, med forbehold for passende sikkerhedsforanstaltninger med hensyn til fysiske personers grundlæggende rettigheder og friheder, herunder tekniske begrænsninger for videreanvendelse samt benyttelse af de mest avancerede sikkerhedsforanstaltninger og foranstaltninger til beskyttelse af privatlivet fred, som f.eks. pseudonymisering eller, i tilfælde hvor anonymisering i væsentlig grad kan påvirke formålet, kryptering.
6. Passende datastyrings- og dataforvaltningspraksisser finder anvendelse på udviklingen af andre højrisiko-AI-systemer end dem, der gør brug af teknikker, der omfatter træning af modeller, således at højrisiko-AI-systemerne er i overensstemmelse med stk. 2.

*Artikel 11*  
*Teknisk dokumentation*

1. Den tekniske dokumentation for et højrisiko-AI-system udarbejdes, inden systemet bringes i omsætning eller tages i brug, og holdes ajour.

Den tekniske dokumentation udarbejdes på en sådan måde, at den påviser, at højrisiko-AI-systemet overholder de krav, der er fastsat i dette kapitel, og således at alle de oplysninger, der er nødvendige for at vurdere AI-systemets overholdelse af disse krav, gives til de nationale kompetente myndigheder og bemyndigede organer. Dokumentationen skal som minimum indeholde de i bilag IV fastsatte elementer.

2. Hvis et højrisiko-AI-system, der er tilknyttet et produkt, der er omfattet af de i bilag II, afsnit A, anførte retsakter, bringes i omsætning eller tages i brug, udarbejdes der en samlet teknisk dokumentation, der indeholder alle de oplysninger, der er anført i bilag IV, samt de oplysninger, der kræves i henhold til disse retsakter.
3. Kommissionen tillægges beføjelse til at vedtage delegerede retsakter, jf. artikel 73, med henblik på at ændre bilag IV, hvis det på baggrund af den tekniske udvikling er nødvendigt for, at den tekniske dokumentation giver alle de oplysninger, der er nødvendige for at vurdere, om systemet opfylder de krav, der er fastsat i dette kapitel.

*Artikel 12*  
*Registrering*

1. Højrisiko-AI-systemer udformes og udvikles på en sådan måde, at hændelser ("logfiler") registreres automatisk, når højrisiko-AI-systemet er i drift. Denne logning er i overensstemmelse med anerkendte standarder eller fælles specifikationer.
2. Logningen sikrer en i forhold til AI-systemets tilsigtede formål passende grad af sporbarhed af systemets funktion gennem hele dets livscyklus.
3. Logningen gør det navnlig muligt at overvåge driften af højrisiko-AI-systemer med hensyn til forekomsten af situationer, der kan medføre, at et AI-system udgør en risiko, jf. artikel 65, stk. 1, eller som kan føre til en væsentlig ændring, samt lette overvågningen efter omsætningen, jf. artikel 61.
4. For så vidt angår de højrisiko-AI-systemer, der er omhandlet i bilag III, punkt 1, litra a), omfatter logningen som minimum:
  - (a) registrering af tidsperioden for hver anvendelse af systemet (startdato og -klokkeslæt samt slutdato og -klokkeslæt for hver anvendelse)
  - (b) den referencedatabase, med hvilken systemet har sammenholdt inputdata
  - (c) de inputdata, som i søgningen har givet et resultat
  - (d) identifikation af de fysiske personer, der er involveret i verificeringen af resultater, jf. artikel 14, stk. 5.

*Artikel 13*  
*Gennemsigtighed og formidling af oplysninger til brugere*

1. Højrisiko-AI-systemer udformes og udvikles på en sådan måde, at deres drift er tilstrækkelig gennemsigtig til, at brugerne kan fortolke systemets output og anvende det korrekt. Der sikres en passende type og grad af gennemsigtighed med henblik på

opfyldelse af de relevante bruger- og udbyderforpligtelser, der er fastsat i dette afsnits kapitel 3.

2. Højrisiko-AI-systemer ledsages af brugsanvisninger i et passende digitalt format eller på anden vis, og disse indeholder kortfattede, fuldstændige, korrekte og klare oplysninger, som er relevante, tilgængelige og forståelige for brugerne.
3. De i stk. 2 omhandlede oplysninger omfatter:
  - (a) identitet på og kontaktoplysninger for udbyderen og dennes eventuelle bemyndigede repræsentant
  - (b) højrisiko-AI-systemets egenskaber, kapacitet og begrænsninger for dets ydeevne, herunder:
    - i) systemets tilsigtede formål
    - ii) det niveau af nøjagtighed, robusthed og cybersikkerhed, jf. artikel 15, i forhold til hvilket højrisiko-AI-systemet er testet og valideret, og som kan forventes, samt alle kendte og forudsigelige omstændigheder, der kan have indvirkning på det forventede niveau af nøjagtighed, robusthed og cybersikkerhed
    - iii) alle kendte eller forudsigelige omstændigheder, som i forbindelse med anvendelse af højrisiko-AI-systemet i overensstemmelse med dets tilsigtede formål eller ved fejlanvendelse, der med rimelighed kan forudses, kan medføre risici for menneskers sundhed og sikkerhed eller grundlæggende rettigheder
    - iv) systemets ydeevne for så vidt angår de personer eller grupper af personer, på hvilke systemet er beregnet til at blive anvendt
    - v) hvis det er relevant, specifikationer for inputdata eller andre relevante oplysninger med hensyn til de anvendte trænings-, validerings- og prøvningsdatasæt under hensyntagen til AI-systemets tilsigtede formål
  - (c) eventuelle ændringer af højrisiko-AI-systemet og dets ydeevne, som udbyderen på forhånd har fastsat på tidspunktet for den indledende overensstemmelsesvurdering
  - (d) foranstaltninger til menneskeligt tilsyn, jf. artikel 14, herunder de tekniske foranstaltninger, der er indført for at lette brugernes fortolkning af AI-systemets output
  - (e) højrisiko-AI-systemets forventede levetid og eventuelle nødvendige vedligeholdelses- og plejeforanstaltninger for at sikre, at AI-systemet fungerer korrekt, herunder med hensyn til softwareopdateringer.

#### *Artikel 14*

##### *Menneskeligt tilsyn*

1. Højrisiko-AI-systemer udformes og udvikles på en sådan måde, herunder med passende menneske-maskine-grænsefladeværktøjer, at fysiske personer kan føre effektivt tilsyn med dem i den periode, hvor AI-systemet er i brug.
2. Menneskeligt tilsyn har til formål at forebygge eller minimere de risici for menneskers sundhed, sikkerhed eller grundlæggende rettigheder, der kan opstå, når et højrisiko-AI-system anvendes i overensstemmelse med dets tilsigtede formål eller

ved fejlanvendelse, der med rimelighed kan forudses, navnlig hvis sådanne risici fortsat består uanset anvendelsen af andre krav, der er fastsat i dette kapitel.

3. Menneskeligt tilsyn sikres ved hjælp af en eller alle af følgende foranstaltninger:
  - (a) menneskeligt tilsyn er fastlagt og, hvis det er teknisk muligt, indbygget i højrisiko-AI-systemet fra udbyderens side, inden systemet bringes i omsætning eller tages i brug
  - (b) menneskeligt tilsyn er fastlagt fra udbyderens side, inden højrisiko-AI-systemet bringes i omsætning eller tages i brug, og er egnet til at blive gennemført af brugeren.
4. De i stk. 3 omhandlede foranstaltninger gør det muligt for de personer, der foretager menneskeligt tilsyn, alt efter omstændighederne at:
  - (a) forstå højrisiko-AI-systemets kapacitet og begrænsninger fuldt ud og være i stand til at overvåge dets drift på behørig vis, således at tegn på uregelmæssigheder, funktionsforstyrrelser og uventet ydeevne kan opdages og afhjælpes så hurtigt som muligt
  - (b) være opmærksomme på den mulige tendens til automatisk eller i overdreven grad af forlade sig på output fra højrisiko-AI-systemet ("automatiseringspartiskhed"), navnlig for så vidt angår højrisiko-AI-systemer, der anvendes til at give oplysninger eller anbefalinger til afgørelser, der skal træffes af fysiske personer
  - (c) kunne fortolke højrisiko-AI-systemets output korrekt under hensyntagen til navnlig systemets egenskaber og de tilgængelige fortolkningsværktøjer og -metoder
  - (d) kunne beslutte ikke at anvende højrisiko-AI-systemet eller på anden måde se bort fra, tilsidesætte eller omgøre output fra højrisiko-AI-systemet i enhver given situation
  - (e) kunne gribe ind i højrisiko-AI-systemets drift eller afbryde systemet ved hjælp af en "stopknap" eller en lignende procedure.
5. For så vidt angår de højrisiko-AI-systemer, der er omhandlet i bilag III, punkt 1, litra a), sikrer de foranstaltninger, der er omhandlet i stk. 3, desuden, at brugeren ikke træffer nogen foranstaltninger eller beslutninger på grundlag af en identifikation, der følger af systemet, medmindre den er blevet verificeret og bekræftet af mindst to fysiske personer.

#### *Artikel 15*

#### *Nøjagtighed, robusthed og cybersikkerhed*

1. Højrisiko-AI-systemer udformes og udvikles på en sådan måde, at de i lyset af deres tilsigtede formål har et passende niveau af nøjagtighed, robusthed og cybersikkerhed og i disse henseender fungerer konsekvent i hele deres livscyklus.
2. Højrisiko-AI-systemers niveau og relevante parametrene med hensyn til nøjagtighed angives i den ledsagende brugsanvisning.
3. Højrisiko-AI-systemer er modstandsdygtige over for fejl, svigt og uoverensstemmelser, der kan forekomme i systemet eller i det miljø, som systemet fungerer i, navnlig på grund af systemets interaktion med fysiske personer eller andre systemer.

4. Højrisiko-AI-systemers robusthed kan opnås ved hjælp af tekniske redundansløsninger, som kan omfatte backupplaner eller fejlsikre planer.
5. De højrisiko-AI-systemer, der fortsætter med at lære efter at være bragt i omsætning eller taget i brug, udvikles på en sådan måde, at det sikres, at eventuelle partiske output som følge af output, der anvendes som input i fremtidig drift ("feedbacksløjfer"), behørigt imødegås ved hjælp af passende afbødende foranstaltninger.
6. Højrisiko-AI-systemer er modstandsdygtige over for uautoriserede tredjeparters forsøg på at ændre deres anvendelse eller ydeevne ved at udnytte systemets sårbarheder.

De tekniske løsninger, der har til formål at sikre cybersikkerhed i forbindelse med højrisiko-AI-systemer, står i et passende forhold til de relevante omstændigheder og risiciene.

De tekniske løsninger til afhjælpning af AI-specifikke sårbarheder omfatter, alt efter hvad der er relevant, foranstaltninger til forebyggelse af og kontrol for angreb, der forsøger at manipulere træningsdatasættet ("dataforgiftning"), input, der har til formål at få modellen til at begå fejl ("fjendtlige eksempler"), eller modelfejl.

### KAPITEL 3

## FORPLIGTELSER FOR UDBYDERE OG BRUGERE AF HØJRISIKO-AI-SYSTEMER OG ANDRE PARTER

### *Artikel 16*

#### *Forpligtelser for udbydere af højrisiko-AI-systemer*

Udbydere af højrisiko-AI-systemer skal:

- (a) sørge for, at deres højrisiko-AI-systemer opfylder de krav, der er fastsat i dette afsnits kapitel 2
- (b) indføre et kvalitetsstyringssystem, der er i overensstemmelse med artikel 17
- (c) udarbejde den tekniske dokumentation for højrisiko-AI-systemet
- (d) opbevare de logfiler, der automatisk genereres af deres højrisiko-AI-systemer, når logfilerne er under deres kontrol
- (e) sørge for, at højrisiko-AI-systemet underkastes den relevante overensstemmelsesvurderingsprocedure, inden systemet bringes i omsætning eller tages i brug
- (f) opfylde registreringsforpligtelsen, jf. artikel 51
- (g) træffe de nødvendige korrigerende foranstaltninger, hvis højrisiko-AI-systemet ikke er i overensstemmelse med de krav, der er fastsat i dette afsnits kapitel 2
- (h) underrette de nationale kompetente myndigheder i de medlemsstater, hvori de har tilgængeliggjort eller ibrugtaget AI-systemet, og, hvis det er relevant, det bemyndigede organ om manglende overensstemmelser og om de korrigerende foranstaltninger, der er truffet
- (i) anbringe CE-mærkningen på deres højrisiko-AI-system for at angive overensstemmelse med denne forordning, jf. artikel 49



- (j) efter anmodning fra en national kompetent myndighed påvise, at højrisiko-AI-systemet opfylder de krav, der er fastsat i dette afsnits kapitel 2.

### *Artikel 17*

#### *Kvalitetsstyringssystem*

1. Udbydere af højrisiko-AI-systemer indfører et kvalitetsstyringssystem, der sikrer overensstemmelse med denne forordning. Systemet dokumenteres på en systematisk og velordnet måde i form af skriftlige politikker, procedurer og anvisninger og skal som minimum omfatte følgende aspekter:
- (a) en strategi for overholdelse af lovgivningen, herunder overholdelse af overensstemmelsesvurderingsprocedurer og procedurer for forvaltning af ændringer af højrisiko-AI-systemet
  - (b) teknikker, procedurer og systematiske foranstaltninger, der anvendes til udformning samt kontrol og verifikation af udformningen af højrisiko-AI-systemet
  - (c) teknikker, procedurer og systematiske foranstaltninger, der anvendes til udvikling, kvalitetskontrol og kvalitetssikring af højrisiko-AI-systemet
  - (d) undersøgelses-, prøvnings- og valideringsprocedurer, der gennemføres før, under og efter udviklingen af højrisiko-AI-systemet, samt den hyppighed, hvormed de gennemføres
  - (e) tekniske specifikationer, herunder standarder, der anvendes, og, hvis de relevante harmoniserede standarder ikke anvendes fuldt ud, de midler, der anvendes for at sikre, at højrisiko-AI-systemet opfylder de krav, der er fastsat i dette afsnits kapitel 2
  - (f) systemer til og procedurer for dataforvaltning, herunder dataindsamling, dataanalyse, datamærkning, datalagring, datafiltrering, dataudvinding, dataaggregering, dataopbevaring og enhver anden handling vedrørende data, som udføres før og med henblik på omsætning eller ibrugtagning af højrisiko-AI-systemer
  - (g) det risikoforvaltningssystem, der er omhandlet i artikel 9
  - (h) oprettelse, implementering og vedligeholdelse af et system til overvågning efter omsætningen, jf. artikel 61
  - (i) procedurer for indberetning af alvorlige hændelser og funktionsfejl, jf. artikel 62
  - (j) håndtering af kommunikation med nationale kompetente myndigheder, kompetente myndigheder, herunder sektorspecifikke myndigheder, der giver eller understøtter adgang til data, bemyndigede organer, andre operatører, kunder eller andre interesserede parter
  - (k) systemer til og procedurer for registrering af al relevant dokumentation og alle relevante oplysninger
  - (l) ressourceforvaltning, herunder foranstaltninger vedrørende forsyningssikkerhed
  - (m) en ansvarlighedsramme, der fastlægger ledelsens og det øvrige personales ansvar med hensyn til alle de aspekter, der er anført i dette stykke.

2. Gennemførelsen af de aspekter, der er omhandlet i stk. 1, står i et rimeligt forhold til størrelsen af udbyderens organisation.
3. For de udbydere, der er kreditinstitutter, der er omfattet af direktiv 2013/36/EU, anses forpligtelsen til at indføre et kvalitetsstyringssystem for at være opfyldt ved overholdelse af reglerne om ordninger, procedurer og mekanismer for intern ledelse, jf. artikel 74 i nævnte direktiv. I den forbindelse tages der hensyn til alle de harmoniserede standarder, der er nævnt i artikel 40 i denne forordning.

#### *Artikel 18*

##### *Forpligtelse til at udarbejde teknisk dokumentation*

1. Udbydere af højrisiko-AI-systemer udarbejder den tekniske dokumentation, der er omhandlet i artikel 11, i overensstemmelse med bilag IV.
2. De udbydere, der er kreditinstitutter, der er omfattet af direktiv 2013/36/EU, vedligeholder den tekniske dokumentation som en del af dokumentationen vedrørende ordningerne, processerne og mekanismerne for intern ledelse, jf. artikel 74 i nævnte direktiv.

#### *Artikel 19*

##### *Overensstemmelsesvurdering*

1. Udbydere af højrisiko-AI-systemer sørger for, at deres systemer underkastes den relevante overensstemmelsesvurderingsprocedure, jf. artikel 43, inden systemerne bringes i omsætning eller tages i brug. Hvis AI-systemets overensstemmelse med de krav, der er fastsat i dette afsnits kapitel 2, er blevet påvist efter denne overensstemmelsesvurdering, udarbejder udbyderen en EU-overensstemmelseserklæring, jf. artikel 48, og anbringer CE-overensstemmelsesmærkningen, jf. artikel 49.
2. For så vidt angår de højrisiko-AI-systemer, der er omhandlet i bilag III, punkt 5, litra b), og som bringes i omsætning eller tages i brug af udbydere, der er kreditinstitutter, der er omfattet af direktiv 2013/36/EU, foretages overensstemmelsesvurderingen som led i den procedure, der er omhandlet i nævnte direktivs artikel 97-101.

#### *Artikel 20*

##### *Automatisk genererede logfiler*

1. Udbydere af højrisiko-AI-systemer opbevarer de logfiler, der genereres automatisk af deres højrisiko-AI-systemer, i det omfang sådanne logfiler er under deres kontrol i kraft af en kontraktmæssig aftale med brugeren eller på anden vis i medfør af loven. Logfilerne opbevares i en periode, der er passende set i lyset af højrisiko-AI-systemets tilsigtede formål og de gældende retlige forpligtelser i henhold til EU-retten eller national ret.
2. Udbydere, som er kreditinstitutter, der er omfattet af direktiv 2013/36/EU, opbevarer de logfiler, der genereres automatisk af deres højrisiko-AI-systemer, som en del af dokumentationen, jf. artikel 74 i nævnte direktiv.

*Artikel 21*  
*Korrigerende foranstaltninger*

De udbydere af højrisiko-AI-systemer, der finder eller har grund til at tro, at et højrisiko-AI-system, som de har bragt i omsætning eller taget i brug, ikke er i overensstemmelse med denne forordning, træffer straks de nødvendige korrigerende foranstaltninger til at bringe det pågældende system i overensstemmelse hermed eller om nødvendigt tilbagetrække eller tilbagekalde det. De underretter distributørerne af det pågældende højrisiko-AI-system og, hvis det er relevant, den bemyndigede repræsentant samt importører herom.

*Artikel 22*  
*Oplysningspligt*

Hvis et højrisiko-AI-system udgør en risiko, jf. artikel 65, stk. 1, og denne risiko er kendt af udbyderen af systemet, underretter udbyderen straks de nationale kompetente myndigheder i de medlemsstater, hvori udbyderen har tilgængeliggjort systemet, og, hvis det er relevant, det bemyndigede organ, der har udstedt et certifikat for højrisiko-AI-systemet, navnlig om den manglende overensstemmelse og om eventuelle korrigerende foranstaltninger, der er truffet.

*Artikel 23*  
*Samarbejde med kompetente myndigheder*

Efter anmodning fra en national kompetent myndighed giver udbydere af højrisiko-AI-systemer denne myndighed al den dokumentation og alle de oplysninger, der er nødvendige for at påvise, at højrisiko-AI-systemet er i overensstemmelse med de krav, der er fastsat i dette afsnits kapitel 2, på et officielt EU-sprog, der er fastsat af den pågældende medlemsstat. Efter begrundet anmodning fra en national kompetent myndighed giver udbydere også denne myndighed adgang til de logfiler, der genereres automatisk af højrisiko-AI-systemet, i det omfang sådanne logfiler er under deres kontrol i kraft af en kontraktmæssig aftale med brugeren eller på anden vis i medfør af loven.

*Artikel 24*  
*Forpligtelser for producenter*

Hvis et højrisiko-AI-system, som er tilknyttet produkter, som de retsakter, der er opført i bilag II, afsnit A, finder anvendelse på, bringes i omsætning eller tages i brug sammen med det pågældende produkt, der er fremstillet i overensstemmelse med disse retsakter og under producentens navn, påtager producenten af produktet sig ansvaret for, at AI-systemet overholder denne forordning, og har, for så vidt angår AI-systemet, de samme forpligtelser, som denne forordning pålægger udbyderen.

*Artikel 25*  
*Bemyndigede repræsentanter*

1. Hvis der ikke kan udpeges en importør, skal udbydere, der er etableret uden for Unionen, inden deres systemer gøres tilgængelige på EU-markedet, ved skriftlig fuldmagt udpege en bemyndiget repræsentant, der er etableret i Unionen.
2. Den bemyndigede repræsentant udfører de opgaver, der er fastsat i den fuldmagt, de har modtaget fra udbyderen. Fuldmagten skal sætte den bemyndigede repræsentant i stand til at udføre følgende opgaver:

- (a) at sørge for at opbevare en kopi af overensstemmelseserklæringen og den tekniske dokumentation, og at disse står til rådighed for de nationale kompetente myndigheder og de nationale myndigheder, der er omhandlet i artikel 63, stk. 7
- (b) efter begrundet anmodning at give de nationale kompetente myndigheder alle de oplysninger og al den dokumentation, der kræves for at påvise, at et højrisiko-AI-system er i overensstemmelse med kravene i dette afsnits kapitel 2, herunder adgang til de logfiler, der genereres automatisk af højrisiko-AI-systemet, i det omfang sådanne logfiler er under udbyderens kontrol i henhold til en kontraktlig ordning med brugeren eller på anden måde i henhold til lovgivningen
- (c) efter begrundet anmodning at samarbejde med de kompetente nationale myndigheder om enhver foranstaltning, som sidstnævnte træffer i forbindelse med højrisiko-AI-systemet.

### *Artikel 26*

#### *Forpligtelser for importører*

1. Importører af højrisiko-AI-systemer skal, før de bringer sådanne systemer i omsætning, sikre, at:
  - (a) udbyderen af dette AI-system har gennemført en passende overensstemmelsesvurderingsprocedure
  - (b) udbyderen har udarbejdet den tekniske dokumentation i overensstemmelse med bilag IV
  - (c) systemet er forsynet med den krævede overensstemmelsesmærkning og er ledsaget af den krævede dokumentation og brugsanvisning.
2. Hvis en importør finder eller har en begrundet formodning om, at et højrisiko-AI-system ikke er i overensstemmelse med denne forordning, må vedkommende ikke bringe dette system i omsætning, før det pågældende AI-system er blevet bragt i overensstemmelse. Hvis højrisiko-AI-systemet udgør en risiko i henhold til artikel 65, stk. 1, skal importøren underrette udbyderen af AI-systemet og markedsovervågningsmyndighederne herom.
3. Importørens navn, registrerede firmanavn eller registrerede varemærke og kontaktadresse skal angives i højrisiko-AI-systemet, eller hvis dette ikke er muligt, på emballagen eller i den dokumentation, der ledsager produktet, alt efter hvad der er relevant.
4. Importører skal, hvor det er relevant, sikre, at opbevarings- og transportbetingelserne for højrisiko-AI-systemer, som de har ansvaret for, ikke bringer dets overholdelse af de væsentlige krav i dette afsnits kapitel 2 i fare.
5. Importører skal efter begrundet anmodning og på et sprog, som den pågældende myndighed let kan forstå, give de nationale kompetente myndigheder alle de oplysninger og al den dokumentation, der kræves for at påvise, at et højrisiko-AI-system er i overensstemmelse med kravene i dette afsnits kapitel 2, herunder adgang til de logfiler, der genereres automatisk af højrisiko-AI-systemet, i det omfang sådanne logfiler er under udbyderens kontrol i henhold til en kontraktlig ordning med brugeren eller på anden måde i henhold til lovgivningen. De skal også samarbejde

med disse myndigheder om enhver foranstaltning, som den nationale kompetente myndighed træffer i forbindelse med dette system.

#### *Artikel 27*

##### *Forpligtelser for distributører*

1. Distributørerne skal, før de gør et højrisiko-AI-system tilgængeligt på markedet, kontrollere, at højrisiko-AI-systemet er forsynet med den krævede CE-overensstemmelsesmærkning, at det ledsages af den krævede dokumentation og brugsanvisning, og at udbyderen og importøren af systemet, alt efter hvad der er relevant, har opfyldt de forpligtelser, der er fastsat i denne forordning.
2. Hvis en distributør finder eller har en begrundet formodning om, at et højrisiko-AI-system ikke er i overensstemmelse med kravene i dette afsnits kapitel 2, må vedkommende ikke gøre dette system tilgængeligt på markedet, før det pågældende system er blevet bragt i overensstemmelse med de nævnte krav. Hvis systemet ydermere udgør en risiko i henhold til artikel 65, stk. 1, skal distributøren underrette udbyderen eller importøren af systemet, alt efter hvad der er relevant, herom.
3. Distributører skal, hvor det er relevant, sikre, at opbevarings- og transportbetingelserne for højrisiko-AI-systemer, som de har ansvaret for, ikke bringer systemets overholdelse af de væsentlige krav i dette afsnits kapitel 2 i fare.
4. Hvis en distributør finder eller har en begrundet formodning om, at et højrisiko-AI-system, som vedkommende har gjort tilgængeligt på markedet, ikke er i overensstemmelse med kravene i dette afsnits kapitel 2, skal vedkommende træffe de nødvendige korrigerende foranstaltninger for at bringe systemet i overensstemmelse med disse krav, trække det tilbage eller kalde det tilbage eller sikre, at udbyderen, importøren eller enhver relevant operatør, alt efter hvad der er relevant, træffer disse korrigerende foranstaltninger. Hvis produktet udgør en risiko i henhold til artikel 65, stk. 1, skal distributøren straks orientere de nationale kompetente myndigheder i de medlemsstater, hvor distributøren har gjort produktet tilgængeligt, herom og give nærmere oplysninger om særlig den manglende overholdelse af lovgivningen og de trufne korrigerende foranstaltninger.
5. Distributører af højrisiko-AI-systemer skal efter begrundet anmodning fra en national kompetent myndighed give denne myndighed alle de oplysninger og al den dokumentation, der kræves for at påvise, at et højrisiko-AI-system er i overensstemmelse med kravene i dette afsnits kapitel 2. Distributørerne skal også samarbejde med den pågældende nationale kompetente myndighed om enhver foranstaltning, der træffes af denne myndighed.

#### *Artikel 28*

##### *Forpligtelser for distributører, importører, brugere eller enhver anden tredjepart*

1. Enhver distributør, importør, bruger eller anden tredjepart anses med henblik på denne forordning for at være en udbyder og er underlagt forpligtelserne for udbydere, jf. artikel 16, i følgende tilfælde:
  - (a) hvis de under eget navn eller varemærke bringer et højrisiko-AI-system i omsætning eller tager det i brug
  - (b) hvis de ændrer det tilsigtede formål med et højrisiko-AI-system, der allerede er bragt i omsætning eller taget i brug

- (c) hvis de foretager en væsentlig ændring af højrisiko-AI-systemet.
2. Hvis de omstændigheder, der er omhandlet i stk. 1, litra b) eller c), indtræffer, anses den udbyder, der oprindeligt bragte AI-systemet i højrisikogruppen i omsætning eller tog det i brug, ikke længere for at være en udbyder i denne forordnings forstand.

#### *Artikel 29*

##### *Forpligtelser for brugere af højrisiko-AI-systemer*

1. Brugere af højrisiko-AI-systemer skal anvende disse systemer i overensstemmelse med den brugsanvisning, der ledsager systemerne, jf. stk. 2 og 5.
2. Forpligtelserne i stk. 1 berører ikke andre brugerforpligtelser i henhold til EU-retten eller national ret eller brugerens mulighed for selv at tilrettelægge sine egne ressourcer og aktiviteter med henblik på at gennemføre de af udbyderen angivne foranstaltninger til menneskeligt tilsyn.
3. Uden at dette berører stk. 1, og i det omfang brugeren udøver kontrol over inputdataene, skal denne bruger sikre, at inputdataene er relevante med hensyn til højrisiko-AI-systemets tilsigtede formål.
4. Brugerne skal overvåge driften af højrisiko-AI-systemet på grundlag af brugsanvisningen. Hvis en bruger har begrundet formodning om, at anvendelsen i overensstemmelse med brugsanvisningen kan medføre, at AI-systemet udgør en risiko som omhandlet i artikel 65, stk. 1, skal vedkommende underrette udbyderen eller distributøren og ophøre med at anvende systemet. Brugeren skal også underrette udbyderen eller distributøren, hvis vedkommende konstaterer alvorlige hændelser eller funktionsfejl, jf. artikel 62, og afbryde anvendelsen af AI-systemet. Hvis brugeren ikke er i stand til at kontakte udbyderen, finder artikel 62 tilsvarende anvendelse.
5. For brugere, som er kreditinstitutter, der er omfattet af direktiv 2013/36/EU, anses overvågningsforpligtelsen i første afsnit for at være opfyldt ved overholdelse af reglerne om ordninger, procedurer og mekanismer for intern ledelse i henhold til artikel 74 i nævnte direktiv.
6. Brugere af højrisiko-AI-systemer skal opbevare de logfiler, der genereres automatisk af det pågældende højrisiko-AI-system, i det omfang sådanne logfiler er under deres kontrol. Logfilerne opbevares i en periode, der er passende i lyset af højrisiko-AI-systemets tilsigtede formål og gældende retlige forpligtelser i henhold til EU-retten eller national ret.  
  
Brugere, som er kreditinstitutter, der er omfattet af direktiv 2013/36/EU, skal opbevare logfilerne som en del af dokumentationen af ordningerne, processerne og mekanismerne for intern ledelse, jf. artikel 74 i nævnte direktiv.
7. Brugere af højrisiko-AI-systemer skal anvende de oplysninger, der angives i henhold til artikel 13, til at opfylde deres forpligtelse til at foretage en konsekvensanalyse vedrørende databeskyttelse i henhold til artikel 35 i forordning (EU) 2016/679 eller artikel 27 i direktiv (EU) 2016/680, hvor det er relevant.

## KAPITEL 4

### BEMYNDIGENDE MYNDIGHEDER OG BEMYNDIGEDE ORGANER

#### *Artikel 30*

##### *Bemyndigende myndigheder*

1. Hver medlemsstat skal udpege eller oprette en bemyndigende myndighed med ansvar for at indføre og gennemføre de nødvendige procedurer for vurdering, udpegelse og bemyndigelse af overensstemmelsesvurderingsorganer og for overvågning heraf.
2. Medlemsstaterne kan udpege et nationalt akkrediteringsorgan, jf. forordning (EF) nr. 765/2008, som bemyndigende myndighed.
3. Bemyndigende myndigheder skal oprettes, organiseres og drives på en sådan måde, at der ikke opstår interessekonflikter med overensstemmelsesvurderingsorganerne, og at der sikres objektivitet og uvildighed i deres aktiviteter.
4. Bemyndigende myndigheder skal være organiseret på en sådan måde, at beslutninger om bemyndigelse af overensstemmelsesvurderingsorganer træffes af kompetente personer, der ikke er identiske med dem, der foretog vurderingen af disse organer.
5. En bemyndigende myndighed må ikke udføre aktiviteter, som udføres af overensstemmelsesvurderingsorganer, eller yde nogen rådgivningsservice på kommercielt eller konkurrencemæssigt grundlag.
6. Bemyndigende myndigheder skal sikre, at de oplysninger, de indhenter, behandles fortroligt.
7. Bemyndigende myndigheder skal have et tilstrækkeligt stort kompetent personale til, at de kan udføre deres opgaver behørigt.
8. De bemyndigende myndigheder skal sikre, at overensstemmelsesvurderingerne udføres på en forholdsmæssig måde for at undgå unødvendige byrder for udbyderne, og at bemyndigede organer udfører deres aktiviteter under behørig hensyntagen til en virksomheds størrelse, til den sektor, som den opererer i, til dens struktur og til det pågældende AI-systems kompleksitet.

#### *Artikel 31*

##### *Ansøgning om bemyndigelse af et overensstemmelsesvurderingsorgan*

1. Overensstemmelsesvurderingsorganer skal indgive en ansøgning om bemyndigelse til den bemyndigende myndighed i den medlemsstat, hvor de er etableret.
2. Ansøgningen om bemyndigelse skal ledsages af en beskrivelse af de overensstemmelsesvurderingsaktiviteter, det eller de overensstemmelsesvurderingsmoduler og de AI-teknologier, som overensstemmelsesvurderingsorganet hævder at være kompetent til, samt af et eventuelt akkrediteringscertifikat udstedt af et nationalt akkrediteringsorgan, hvori det attesteres, at overensstemmelsesvurderingsorganet opfylder kravene i artikel 33. Alle gyldige dokumenter vedrørende eksisterende udpegelser af det ansøgende bemyndigede organ i henhold til anden EU-harmoniseringslovgivning skal tilføjes.
3. Hvis det pågældende overensstemmelsesvurderingsorgan ikke kan forelægge et akkrediteringscertifikat, skal det forelægge den bemyndigende myndighed den dokumentation, der er nødvendig for at kontrollere, anerkende og regelmæssigt

overvåge, at det opfylder kravene i artikel 33. For bemyndigede organer, der er udpeget i henhold til anden EU-harmoniseringslovgivning, kan alle dokumenter og attester, der er knyttet til disse udpegelser, alt efter hvad der er relevant, anvendes til at understøtte deres udpegelsesprocedure i henhold til denne forordning.

#### *Artikel 32* *Bemyndigelsesprocedure*

1. De bemyndigende myndigheder må kun bemyndige overensstemmelsesvurderingsorganer, som opfylder kravene i artikel 33.
2. De bemyndigende myndigheder underretter Kommissionen og de øvrige medlemsstater ved hjælp af det elektroniske notifikationsværktøj, der er udviklet og forvaltes af Kommissionen.
3. Notifikationen skal indeholde fyldestgørende oplysninger om overensstemmelsesvurderingsaktiviteterne, det eller de pågældende overensstemmelsesvurderingsmoduler og de pågældende AI-teknologier.
4. Det pågældende overensstemmelsesvurderingsorgan må kun udøve aktiviteter som bemyndiget organ, hvis Kommissionen og de øvrige medlemsstater ikke har gjort indsigelse inden for to uger efter en bemyndigelse.
5. De bemyndigende myndigheder skal underrette Kommissionen og de øvrige medlemsstater om enhver relevant efterfølgende ændring af bemyndigelsen.

#### *Artikel 33* *Bemyndigede organer*

1. De bemyndigede organer skal verificere, at højrisiko-AI-systemer er i overensstemmelse med de overensstemmelsesvurderingsprocedurer, der er omhandlet i artikel 43.
2. De bemyndigede organer skal opfylde de organisatoriske krav samt de kvalitetsstyrings-, ressource- og procedurekrav, der er nødvendige for at kunne udføre disse opgaver.
3. De bemyndigede organers organisationsstruktur, ansvarsfordeling, rapporteringsveje og drift skal være af en sådan art, at de sikrer, at der er tillid til de bemyndigede organers arbejde og til resultaterne af de bemyndigede organers overensstemmelsesvurderingsaktiviteter.
4. De bemyndigede organer skal være uafhængige af udbyderen af det højrisiko-AI-system, i forbindelse med hvilket de udfører overensstemmelsesvurderingsaktiviteter. Bemyndigede organer skal også være uafhængige af alle andre operatører, der har en økonomisk interesse i det vurderede højrisiko-AI-system, og af enhver konkurrent til udbyderen.
5. De bemyndigede organer skal være organiseret og arbejde på en sådan måde, at der i deres aktiviteter sikres uafhængighed, objektivitet og uvildighed. De bemyndigede organer skal dokumentere og gennemføre en struktur og procedurer til sikring af uvildighed og til fremme og anvendelse af principperne om uvildighed i hele deres organisation, hos alt deres personale og i alle deres vurderingsaktiviteter.
6. De bemyndigede organer skal have indført dokumenterede procedurer, der sikrer, at personale, udvalg, dattervirksomheder, underentreprenører og eventuelle tilknyttede



organer eller personalet i eksterne organer behandler de oplysninger, som de kommer i besiddelse af under udførelsen af overensstemmelsesvurderingsaktiviteterne, fortroligt, medmindre videregivelse af oplysningerne er fastsat ved lov. De bemyndigede organers personale har tavshedspligt med hensyn til alle oplysninger, det kommer i besiddelse af ved udførelsen af dets opgaver i henhold til denne forordning, undtagen over for de bemyndigende myndigheder i den medlemsstat, hvor aktiviteterne udføres.

7. De bemyndigede organer skal have indført procedurer, der sætter dem i stand til at udføre deres aktiviteter under behørig hensyntagen til en virksomheds størrelse, til den sektor, som den opererer inden for, til dens struktur og til, hvor kompleks det pågældende AI-system er.
8. De bemyndigede organer skal tegne en passende ansvarsforsikring for deres overensstemmelsesvurderingsaktiviteter, medmindre den pågældende medlemsstat er ansvarlig i henhold til national ret, eller medlemsstaten er direkte ansvarlig for overensstemmelsesvurderingen.
9. De bemyndigede organer skal være i stand til at udføre alle de opgaver, som de pålægges ved denne forordning, med den størst mulig faglige integritet og den nødvendige kompetence på det specifikke område, uanset om disse opgaver udføres af bemyndigede organer selv eller på deres vegne og på deres ansvar.
10. De bemyndigede organer skal have tilstrækkelige interne kompetencer til effektivt at kunne evaluere de opgaver, der udføres af eksterne parter på deres vegne. Derfor skal det bemyndigede organ til enhver tid og for hver overensstemmelsesvurderingsprocedure og hver type højrisiko-AI-system, som det er udpeget til, have permanent adgang til tilstrækkeligt administrativt, teknisk og videnskabeligt personale med erfaring og viden vedrørende de relevante AI-teknologier, data, databehandling og kravene i dette afsnits kapitel 2.
11. De bemyndigede organer skal deltage i det koordinerende arbejde, jf. artikel 38. De skal også deltage direkte eller være repræsenteret i de europæiske standardiseringsorganisationer eller sikre, at de har et ajourført kendskab til de relevante standarder.
12. De bemyndigede organer skal stille al relevant dokumentation til rådighed og efter anmodning forelægge denne, herunder udbyderens dokumentation, for den bemyndigende myndighed, der er omhandlet i artikel 30, så den kan udføre sine vurderings-, udpegelses-, bemyndigelses-, tilsyns- og overvågningsaktiviteter og fremme vurderingen som anført i dette kapitel.

#### *Artikel 34*

##### *Dattervirksomheder og underentreprise i tilknytning til bemyndigede organer*

1. Hvis et bemyndiget organ giver bestemte opgaver i forbindelse med overensstemmelsesvurderingen i underentreprise eller anvender en dattervirksomhed, skal det sikre, at underentreprenøren eller dattervirksomheden opfylder kravene i artikel 33, og underrette den bemyndigende myndighed herom.
2. De bemyndigede organer har det fulde ansvar for de opgaver, der udføres af underentreprenører eller dattervirksomheder, uanset hvor disse er etableret.
3. Aktiviteter må kun gives i underentreprise eller udføres af en dattervirksomhed, hvis udbyderen har givet sit samtykke hertil.

4. De bemyndigede organer skal kunne stille de relevante dokumenter vedrørende vurderingen af underentreprenørens eller dattervirksomhedens kvalifikationer og det arbejde, som de har udført i henhold til denne forordning, til rådighed for den bemyndigende myndighed.

#### *Artikel 35*

##### *Identifikationsnumre for og lister over bemyndigede organer, der er udpeget i henhold til denne forordning*

1. Kommissionen tildeler hvert bemyndiget organ et identifikationsnummer. Hvert bemyndiget organ tildeles kun ét nummer, også selv om organet er bemyndiget i henhold til flere EU-retsakter.
2. Kommissionen offentliggør listen over organer, der er bemyndiget i henhold til denne forordning, herunder de identifikationsnumre, som de er blevet tildelt, og de aktiviteter, for hvilke de er bemyndiget. Kommissionen sikrer, at listen ajourføres.

#### *Artikel 36*

##### *Ændringer af bemyndigelser*

1. Hvis en bemyndigende myndighed har mistanke om eller er blevet orienteret om, at et bemyndiget organ ikke længere opfylder kravene i artikel 33, eller at det ikke opfylder sine forpligtelser, skal den myndighed hurtigst muligt undersøge sagen med den størst mulige omhu. I den forbindelse skal den underrette det berørte bemyndigede organ om sine indvendinger og giver det mulighed for at tilkendegive sine synspunkter. Hvis en bemyndigende myndighed konkluderer, at det undersøgte bemyndigede organ ikke længere opfylder kravene i artikel 33, eller at det ikke opfylder sine forpligtelser, skal den begrænse, suspendere eller inddrage bemyndigelsen, alt efter hvad der er mest hensigtsmæssigt, og afhængigt af hvor alvorlig den manglende opfyldelse af kravene eller forpligtelserne er. Den skal derudover straks underrette Kommissionen og de øvrige medlemsstater herom.
2. Hvis en bemyndigelse begrænses, suspenderes eller inddrages, eller hvis det bemyndigede organ har indstillet sine aktiviteter, skal den bemyndigende myndighed træffe de nødvendige foranstaltninger for at sikre, at dette bemyndigede organs sager enten overtages af et andet bemyndiget organ eller står til rådighed for de ansvarlige bemyndigende myndigheder efter disses anmodning.

#### *Artikel 37*

##### *Anfægtelse af bemyndigede organers kompetence*

1. Kommissionen undersøger om nødvendigt alle tilfælde, hvor der er grund til at betvivle, at et bemyndiget organ opfylder kravene i artikel 33.
2. Den bemyndigende myndighed skal efter anmodning forelægge Kommissionen alle relevante oplysninger vedrørende bemyndigelsen af det pågældende bemyndigede organ.
3. Kommissionen sikrer, at alle fortrolige oplysninger, som den indhenter som led i sine undersøgelser i henhold til denne artikel, behandles fortroligt.
4. Hvis Kommissionen konstaterer, at et bemyndiget organ ikke eller ikke længere opfylder kravene i artikel 33, vedtager den en begrundet afgørelse, der pålægger den bemyndigende medlemsstat at træffe de nødvendige korrigerende foranstaltninger,

herunder om nødvendigt inddragelse af bemyndigelsen. Denne gennemførelsesretsakt vedtages efter undersøgelsesproceduren, jf. artikel 74, stk. 2.

#### *Artikel 38*

##### *Koordinering af bemyndigede organer*

1. Kommissionen sikrer, at der på de områder, der er omfattet af denne forordning, etableres passende koordinering og samarbejde mellem de bemyndigede organer, der er aktive inden for overensstemmelsesvurderingsprocedurer for AI-systemer i henhold til denne forordning, og at det i form af en sektorspecifik gruppe af bemyndigede organer fungerer korrekt.
2. Medlemsstaterne skal sørge for, at de organer, de har bemyndiget, deltager i arbejdet i denne gruppe enten direkte eller gennem udpegede repræsentanter.

#### *Artikel 39*

##### *Tredjelandes overensstemmelsesvurderingsorganer*

Overensstemmelsesvurderingsorganer, der er oprettet i henhold til lovgivningen i et tredjeland, med hvilket Unionen har indgået en aftale, kan godkendes til at udføre bemyndigede organers aktiviteter i henhold til denne forordning.

## **KAPITEL 5**

### **STANDARDS, OVERENSSTEMMELSESVURDERING, CERTIFIKATER, REGISTRERING**

#### *Artikel 40*

##### *Harmoniserede standarder*

Højrisiko-AI-systemer, som er i overensstemmelse med harmoniserede standarder eller dele heraf, hvis referencer er offentliggjort i Den Europæiske Unions Tidende, formodes at være i overensstemmelse med de krav, der er fastsat i dette afsnits kapitel 2, for så vidt de nævnte standarder omfatter disse krav.

#### *Artikel 41*

##### *Fælles specifikationer*

1. I tilfælde, hvor der ikke findes harmoniserede standarder som omhandlet i artikel 40, eller hvis Kommissionen finder, at de relevante harmoniserede standarder er utilstrækkelige, eller at der er behov for at tage hensyn til specifikke betænkeligheder vedrørende sikkerhed eller grundlæggende rettigheder, kan Kommissionen ved hjælp af gennemførelsesretsakter vedtage fælles specifikationer for de krav, der er fastsat i dette afsnits kapitel 2. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 74, stk. 2.
2. Kommissionen indsamler i forbindelse med udarbejdelsen af de fælles specifikationer, der er omhandlet i stk. 1, synspunkter fra relevante organer eller ekspertgrupper, der er nedsat i henhold til relevant sektorspecifik EU-ret.
3. Højrisiko-AI-systemer, som er i overensstemmelse med de fælles specifikationer, der er omhandlet i stk. 1, formodes at være i overensstemmelse med de krav, der er

fastsat i dette afsnits kapitel 2, for så vidt de nævnte fælles specifikationer omfatter disse krav.

4. I tilfælde, hvor udbydere ikke overholder de fælles specifikationer, der er omhandlet i stk. 1, skal de behørigt begrunde, at de har indført tekniske løsninger, der mindst svarer hertil.

#### *Artikel 42*

##### *Formodning om overensstemmelse med visse krav*

1. Under hensyntagen til deres tilsigtede formål formodes højrisiko-AI-systemer, der er blevet trænet og testet med data vedrørende de specifikke geografiske, adfærdsmæssige og funktionelle rammer, som systemet skal anvendes inden for, at opfylde kravet i artikel 10, stk. 4.
2. Højrisiko-AI-systemer, der er certificeret, eller for hvilke der er udstedt en overensstemmelseserklæring i henhold til en cybersikkerhedsordning i henhold til Europa-Parlamentets og Rådets forordning (EU) 2019/881<sup>63</sup>, og hvis referencer er offentliggjort i Den Europæiske Unions Tidende, formodes at være i overensstemmelse med cybersikkerhedskravene i nærværende forordnings artikel 15, såfremt cybersikkerhedsattesten eller overensstemmelseserklæringen eller dele heraf dækker disse krav.

#### *Artikel 43*

##### *Overensstemmelsesvurdering*

1. Hvad angår højrisiko-AI-systemer, der er anført i bilag III, punkt 1, skal udbyderen, såfremt denne ved påvisningen af, at et højrisiko-AI-system opfylder kravene i dette afsnits kapitel 2, har anvendt harmoniserede standarder som omhandlet i artikel 40 eller, hvor det er relevant, fælles specifikationer som omhandlet i artikel 41, anvende en af følgende procedurer:
  - (a) overensstemmelsesvurderingsproceduren på grundlag af intern kontrol som omhandlet i bilag VI
  - (b) overensstemmelsesvurderingsproceduren på grundlag af vurdering af kvalitetsstyringssystemet og vurdering af den tekniske dokumentation med inddragelse af et bemyndiget organ, jf. bilag VII.

Hvis udbyderen ved påvisning af et højrisiko-AI-systems overensstemmelse med kravene i dette afsnits kapitel 2 ikke har anvendt eller kun delvist har anvendt harmoniserede standarder som omhandlet i artikel 40, eller hvis sådanne harmoniserede standarder ikke findes, og der ikke foreligger fælles specifikationer som omhandlet i artikel 41, skal udbyderen følge den overensstemmelsesvurderingsprocedure, der er anført i bilag VII.

Med henblik på den overensstemmelsesvurderingsprocedure, der er omhandlet i bilag VII, kan udbyderen vælge hvilket som helst af de bemyndigede organer. Hvis systemet er beregnet til at blive taget i brug af retshåndhævende myndigheder,

---

<sup>63</sup> Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 1).

indvandringsmyndigheder, asylmyndigheder eller EU's institutioner, organer eller agenturer, fungerer den markedsovervågningsmyndighed, der er omhandlet i artikel 63, stk. 5 eller 6, alt efter hvad der er relevant, imidlertid som bemyndiget organ.

2. Hvad angår de højrisiko-AI-systemer, der er omhandlet i bilag III, punkt 2-8, skal udbyderne følge overensstemmelsesvurderingsproceduren på grundlag af intern kontrol som omhandlet i bilag VI, som ikke foreskriver inddragelse af et bemyndiget organ. Hvad angår de højrisiko-AI-systemer, der er omhandlet i bilag III, punkt 5, litra b), og som bringes i omsætning eller tages i brug af kreditinstitutter, der er omfattet af direktiv 2013/36/EU, foretages overensstemmelsesvurderingen som led i den procedure, der er omhandlet i nævnte direktivs artikel 97-101.
3. For højrisiko-AI-systemer, som de retsakter, der er opført i bilag II, afsnit A, finder anvendelse på, skal udbyderen følge den relevante overensstemmelsesvurdering som krævet i henhold til disse retsakter. Kravene i nærværende afsnits kapitel 2 finder anvendelse på disse højrisiko-AI-systemer og skal indgå i den nævnte vurdering. Punkt 4.3, 4.4 og 4.5 samt femte afsnit i punkt 4.6 i bilag VII finder også anvendelse.

Med henblik på denne vurdering har bemyndigede organer, der er blevet bemyndiget i henhold til disse retsakter, ret til at kontrollere, at højrisiko-AI-systemerne opfylder kravene i nærværende afsnits kapitel 2, forudsat at disse bemyndigede organers overholdelse af kravene i artikel 33, stk. 4, 9 og 10, er blevet vurderet i forbindelse med bemyndigelsesproceduren i henhold til disse retsakter.

Hvis de retsakter, der er opført i bilag II, afsnit A, giver producenten af produktet mulighed for at fravælge en af tredjepart udført overensstemmelsesvurdering, forudsat at producenten har anvendt alle de harmoniserede standarder, der omfatter alle de relevante krav, kan producenten kun gøre brug af denne mulighed, hvis vedkommende også har anvendt harmoniserede standarder eller, hvor det er relevant, fælles specifikationer som omhandlet i artikel 41, der omfatter kravene i dette afsnits kapitel 2.

4. Højrisiko-AI-systemer skal underkastes en ny overensstemmelsesvurderingsprocedure, hvis de ændres væsentligt, uanset om det ændrede system skal videredistribueres eller fortsat anvendes af den nuværende bruger.

For højrisiko-AI-systemer, der bliver ved med at lære efter at være bragt i omsætning eller taget i brug, udgør ændringer af højrisiko-AI-systemet og dets ydeevne, som udbyderen på forhånd har fastlagt på tidspunktet for den indledende overensstemmelsesvurdering, og som er en del af oplysningerne i den tekniske dokumentation, jf. bilag IV, punkt 2, litra f), ikke en væsentlig ændring.

5. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 73 for at ajourføre bilag VI og bilag VII med henblik på at indføre elementer i overensstemmelsesvurderingsprocedurerne, der viser sig at blive nødvendige i lyset af den tekniske udvikling.
6. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter for at ændre stk. 1 og 2 med henblik på at underkaste de i bilag III, punkt 2-8, omhandlede højrisiko-AI-systemer overensstemmelsesvurderingsproceduren i bilag VII eller dele heraf. Kommissionen vedtager sådanne delegerede retsakter under hensyntagen til effektiviteten af overensstemmelsesvurderingsproceduren på grundlag af intern kontrol, jf. bilag VI, med hensyn til at forebygge eller minimere de risici for

sundhed, sikkerhed og beskyttelsen af de grundlæggende rettigheder, som sådanne systemer medfører, samt hvorvidt de bemyndigede organer har adgang til tilstrækkelig kapacitet og ressourcer.

*Artikel 44  
Certifikater*

1. Certifikater, der udstedes af bemyndigede organer i overensstemmelse med bilag VII, skal udfærdiges på et officielt EU-sprog fastsat af den medlemsstat, hvor det bemyndigede organ er etableret, eller på et officielt EU-sprog, som det bemyndigede organ kan acceptere.
2. Certifikaterne skal være gyldige i den periode, der er angivet deri, dog højst i fem år. På udbyderens anmodning kan et certifikats gyldighedsperiode forlænges med yderligere perioder på hver højst fem år på grundlag af en fornyet vurdering i overensstemmelse med de gældende overensstemmelsesvurderingsprocedurer.
3. Hvis et bemyndiget organ fastslår, at et AI-system ikke længere opfylder kravene i dette afsnits kapitel 2, skal organet suspendere eller inddrage det udstedte certifikat eller begrænser det under iagttagelse af proportionalitetsprincippet, medmindre udbyderen af systemet gennem passende korrigerende handlinger og inden for en passende frist fastsat af det bemyndigede organ sikrer, at kravene opfyldes. Det bemyndigede organ skal begrunde sin beslutning.

*Artikel 45  
Appel af afgørelser truffet af bemyndigede organer*

Medlemsstaterne skal sikre, at det bemyndigede organs afgørelser kan appelleres af parter, der har en legitim interesse i den pågældende afgørelse.

*Artikel 46  
Oplysningskrav for bemyndigede organer*

1. De bemyndigede organer skal oplyse den bemyndigende myndighed om følgende:
  - (a) alle EU-vurderingscertifikater for teknisk dokumentation, eventuelle tillæg til disse certifikater og godkendelser af kvalitetsstyringssystemer, der er udstedt i overensstemmelse med kravene i bilag VII
  - (b) alle afslag på, begrænsninger af, suspensioner af eller inddragelser af EU-vurderingscertifikater for teknisk dokumentation eller godkendelser af kvalitetsstyringssystemer udstedt i overensstemmelse med kravene i bilag VII
  - (c) alle forhold, der har indflydelse på omfanget af eller betingelserne for bemyndigelsen
  - (d) alle anmodninger om oplysninger om overensstemmelsesvurderingsaktiviteter, som de har modtaget fra markedsovervågningsmyndighederne
  - (e) efter anmodning, overensstemmelsesvurderingsaktiviteter, der er udført inden for det område, hvor de er bemyndiget, og enhver anden aktivitet, der er udført, herunder grænseoverskridende aktiviteter og underentreprise.
2. Hvert bemyndiget organ skal underrette de øvrige bemyndigede organer om:

- (a) afviste, suspenderede eller tilbagekaldte godkendelser af kvalitetsstyringssystemer samt, efter anmodning, udstedte godkendelser af kvalitetsstyringssystemer
  - (b) EU-vurderingscertifikater for teknisk dokumentation eller tillæg hertil, som det har afvist, inddraget, suspenderet eller på anden måde begrænset, og, efter anmodning, de certifikater og/eller tillæg hertil, som det har udstedt.
3. Hvert bemyndiget organ skal give de øvrige bemyndigede organer, som udfører lignende overensstemmelsesvurderingsaktiviteter vedrørende de samme AI-teknologier, relevante oplysninger om spørgsmål vedrørende negative og, efter anmodning, positive overensstemmelsesvurderingsresultater.

#### *Artikel 47*

#### *Undtagelse fra overensstemmelsesvurderingsprocedure*

1. Uanset artikel 43 kan enhver markedsovervågningsmyndighed tillade, at specifikke højrisiko-AI-systemer bringes i omsætning eller tages i brug på den pågældende medlemsstats område af ekstraordinære hensyn til den offentlige sikkerhed eller beskyttelse af menneskers liv og sundhed, miljøbeskyttelse eller beskyttelse af centrale industrielle og infrastrukturmæssige aktiver. Tilladelsen skal gælde for en begrænset periode, mens de nødvendige overensstemmelsesvurderingsprocedurer gennemføres, og skal ophøre, når disse procedurer er afsluttet. Gennemførelsen af disse procedurer skal ske uden unødigt forsinkelse.
2. Den i stk. 1 omhandlede tilladelse må kun udstedes, hvis markedsovervågningsmyndigheden konkluderer, at højrisiko-AI-systemet opfylder kravene i dette afsnits kapitel 2. Markedsovervågningsmyndigheden skal underrette Kommissionen og de øvrige medlemsstater om enhver tilladelse, der udstedes i henhold til stk. 1.
3. Hvis der ikke inden for 15 kalenderdage efter modtagelsen af de i stk. 2 omhandlede oplysninger er blevet gjort indsigelse af en medlemsstat eller Kommissionen mod en tilladelse, der i henhold til stk. 1 er udstedt af en medlemsstats markedsovervågningsmyndighed, anses denne tilladelse for at være berettiget.
4. Hvis en medlemsstat inden for 15 kalenderdage efter modtagelsen af den i stk. 2 omhandlede underretning gør indsigelse mod en tilladelse, der er udstedt af en markedsovervågningsmyndighed i en anden medlemsstat, eller hvis Kommissionen finder, at tilladelsen er i strid med EU-retten, eller at medlemsstaternes konklusion vedrørende systemets opfyldelse af kravene, jf. stk. 2, er ubegrundet, drøfter Kommissionen straks spørgsmålet med den relevante medlemsstat, og i denne forbindelse høres den eller de berørte operatører, som gives mulighed for at fremsætte deres synspunkter. På denne baggrund træffer Kommissionen afgørelse om, hvorvidt tilladelsen er berettiget eller ej. Kommissionen retter sin afgørelse til den pågældende medlemsstat og den eller de relevante operatører.
5. Hvis tilladelsen anses for at være uberettiget, skal den inddrages af markedsovervågningsmyndigheden i den pågældende medlemsstat.
6. Uanset stk. 1-5 finder artikel 59 i forordning (EU) 2017/745 og artikel 54 i forordning (EU) 2017/746 også anvendelse på højrisiko-AI-systemer, der er beregnet til at blive anvendt som sikkerhedskomponenter i udstyr, eller som i selv er udstyr, der er omfattet af forordning (EU) 2017/745 og forordning (EU) 2017/746, for så

vidt angår undtagelse fra overensstemmelsesvurderingen af opfyldelsen af kravene i dette afsnits kapitel 2.

#### *Artikel 48*

##### *EU-overensstemmelseserklæring*

1. Udbyderen skal udarbejde en skriftlig EU-overensstemmelseserklæring for hvert AI-system og opbevare den, så den i ti år efter, at AI-systemet er blevet bragt i omsætning eller taget i brug, står til rådighed for de nationale kompetente myndigheder. Det skal af EU-overensstemmelseserklæringen fremgå, hvilket AI-system den vedrører. Et eksemplar af EU-overensstemmelseserklæringen skal efter anmodning fremsendes til de relevante nationale kompetente myndigheder.
2. Det skal af EU-overensstemmelseserklæringen fremgå, at det pågældende højrisiko-AI-system opfylder kravene i dette afsnits kapitel 2. EU-overensstemmelseserklæringen skal indeholde de oplysninger, der er anført i bilag V, og skal oversættes til det eller de officielle EU-sprog, der kræves af den eller de medlemsstater, hvor højrisiko-AI-systemet gøres tilgængeligt.
3. For højrisiko-AI-systemer, der er omfattet af anden EU-harmoniseringslovgivning, i henhold til hvilken der også kræves en EU-overensstemmelseserklæring, udarbejdes der en enkelt EU-overensstemmelseserklæring for al EU-lovgivning, der finder anvendelse på højrisiko-AI-systemet. Erklæringen skal indeholde alle oplysninger, der er påkrævet for at identificere, hvilken EU-harmoniseringslovgivning erklæringen vedrører.
4. Ved at udarbejde EU-overensstemmelseserklæringen står udbyderen inde for, at kravene i dette afsnits kapitel 2 opfyldes. Udbyderen skal sørge for at holde EU-overensstemmelseserklæringen ajour, hvis det er relevant.
5. Kommissionen tillægges beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 73 for at ajourføre indholdet af EU-overensstemmelseserklæringen, jf. bilag V, med henblik på at indføre elementer, der viser sig at blive nødvendige på baggrund af den tekniske udvikling.

#### *Artikel 49*

##### *CE-overensstemmelsesmærkning*

1. CE-mærkningen skal i tilknytning til højrisiko-AI-systemer anbringes synligt, letlæseligt og således, at den ikke kan slettes. Hvis højrisiko-AI-systemet er af en sådan art, at dette ikke er muligt eller berettiget, anbringes mærkningen på emballagen eller i den medfølgende dokumentation, alt efter hvad der er relevant.
2. CE-mærkningen, jf. nærværende artikels stk. 1, er underkastet de generelle principper i artikel 30 i forordning (EF) nr. 765/2008.
3. Hvor det er relevant, skal CE-mærkningen følges af identifikationsnummeret for det bemyndigede organ, der er ansvarligt for overensstemmelsesvurderingsprocedurene i artikel 43. Identifikationsnummeret skal også fremgå af salgsfremmende materiale, som nævner, at højrisiko-AI-systemet opfylder kravene til CE-mærkning.



*Artikel 50*  
*Opbevaring af dokumentation*

Udbyderen skal i ti år efter, at AI-systemet er blevet bragt i omsætning eller taget i brug, kunne forelægge de nationale kompetente myndigheder:

- (a) den i artikel 11 omhandlede tekniske dokumentation
- (b) dokumentation vedrørende det i artikel 17 omhandlede kvalitetsstyringssystem
- (c) dokumentation vedrørende ændringer, der er godkendt af bemyndigede organer, hvor dette er relevant
- (d) afgørelser og andre dokumenter udstedt af de bemyndigede organer, hvor dette er relevant
- (e) den i artikel 48 omhandlede EU-overensstemmelseserklæring.

*Artikel 51*  
*Registrering*

Inden et højrisiko-AI-system som omhandlet i artikel 6, stk. 2, bringes i omsætning eller tages i brug, skal udbyderen eller, hvor det er relevant, den bemyndigede repræsentant registrere systemet i den EU-database, der er omhandlet i artikel 60.

## AFSNIT IV

### GENNEMSIGTIGHEDSFORPLIGTELSE FOR VISSE AI-SYSTEMER

*Artikel 52*  
*Gennemsigtighedsforpligtelser for visse AI-systemer*

1. Udbydere skal sikre, at AI-systemer, der er beregnet til at interagere med fysiske personer, udformes og udvikles på en sådan måde, at fysiske personer oplyses om, at de interagerer med et AI-system, medmindre dette er indlysende ud fra omstændighederne og anvendelsessammenhængen. Denne forpligtelse finder ikke anvendelse på AI-systemer, der ved lov er godkendt til at afsløre, forebygge, efterforske og retsforfølge strafbare handlinger, medmindre disse systemer er tilgængelige for offentligheden med henblik på at anmelde strafbare handlinger.
2. Brugere af et system til følelsesgenkendelse eller et system til biometrisk kategorisering skal oplyse de fysiske personer, der er eksponeret for systemet, om anvendelsen af systemet. Denne forpligtelse finder ikke anvendelse på AI-systemer, der anvendes til biometrisk kategorisering, og som i henhold til lovgivningen er godkendt til at afsløre, forebygge og efterforske strafbare handlinger.
3. Brugere af et AI-system, der genererer eller manipulerer billed-, lyd- eller videoindhold, der i væsentlig grad ligner faktiske personer, genstande, steder eller andre enheder eller begivenheder, og som fejlagtigt vil fremstå ægte eller sandfærdigt ("deepfake"), skal oplyse, at indholdet er blevet genereret kunstigt eller manipuleret.

Første afsnit finder dog ikke anvendelse, hvis anvendelsen er tilladt ved lov med henblik på at afsløre, forebygge, efterforske og retsforfølge strafbare handlinger, eller hvis anvendelsen er nødvendig for udøvelsen af ytringsfriheden og retten til frihed for kunst og videnskab, der er sikret ved Den Europæiske Unions charter om

grundlæggende rettigheder, og giver passende garantier for tredjemands rettigheder og friheder.

4. Stk. 1, 2 og 3 berører ikke kravene og forpligtelserne i denne forordnings afsnit III.

## AFSNIT V

# FORANSTALTNINGER TIL STØTTE FOR INNOVATION

### *Artikel 53*

#### *Reguleringsmæssige sandkasser for kunstig intelligens*

1. Reguleringsmæssige sandkasser for kunstig intelligens, der er oprettet af en eller flere medlemsstaters kompetente myndigheder eller Den Europæiske Tilsynsførende for Databeskyttelse, skal tilvejebringe et kontrolleret miljø, der letter udviklingen, prøvningen og valideringen af innovative AI-systemer i et begrænset tidsrum, inden de bringes i omsætning eller tages i brug i henhold til en specifik plan. Dette skal ske under de kompetente myndigheders direkte tilsyn og vejledning med henblik på at sikre overholdelse af kravene i denne forordning og, hvor det er relevant, anden EU-lovgivning og national lovgivning, som der føres tilsyn med i sandkassen.
2. I det omfang de innovative AI-systemer omfatter behandling af personoplysninger eller på anden måde henhører under tilsynsområdet for andre nationale myndigheder eller kompetente myndigheder, der giver eller understøtter adgang til data, skal medlemsstaterne sikre, at de nationale databeskyttelsesmyndigheder og disse andre nationale myndigheder er tilknyttet driften af den reguleringsmæssige sandkasse for kunstig intelligens.
3. De reguleringsmæssige sandkasser for kunstig intelligens berører ikke de kompetente myndigheders tilsynsbeføjelser eller korrigerende beføjelser. Enhver væsentlig risiko for sundheden, sikkerheden eller de grundlæggende rettigheder, der konstateres under udviklingen og afprøvningen af sådanne systemer, skal afbødes straks, og hvis dette ikke er muligt, skal udviklings- og prøvningsprocessen suspenderes, indtil en sådan afbødning finder sted.
4. Deltagerne i den reguleringsmæssige sandkasse for kunstig intelligens forbliver ansvarlige i henhold til EU's og medlemsstaternes gældende ansvarslovgivning for enhver skade, der påføres tredjeparter som følge af forsøg i sandkassen.
5. De af medlemsstaternes kompetente myndigheder, der har etableret reguleringsmæssige sandkasser for kunstig intelligens, skal koordinere deres aktiviteter og samarbejde inden for rammerne af Det Europæiske Udvalg for Kunstig Intelligens. De skal forelægge årlige rapporter for udvalget og Kommissionen om resultaterne af gennemførelsen af disse ordninger, herunder god praksis, indhøstede erfaringer og anbefalinger vedrørende deres udformning og, hvor det er relevant, vedrørende anvendelsen af denne forordning og anden EU-lovgivning, der overvåges inden for sandkassen.
6. De nærmere bestemmelser og betingelserne for driften af de reguleringsmæssige sandkasser for kunstig intelligens, herunder udvælgelseskriterierne og proceduren for ansøgning, udvælgelse, deltagelse og udtræden af sandkassen, samt deltagernes rettigheder og forpligtelser fastsættes i gennemførelsesretsakter. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 74, stk. 2.

#### Artikel 54

#### *Viderebehandling af personoplysninger med henblik på udvikling af visse AI-systemer i offentlighedens interesse i den reguleringsmæssige sandkasse for kunstig intelligens*

1. I den reguleringsmæssige sandkasse for kunstig intelligens behandles personoplysninger, der er lovligt indsamlet til andre formål, med henblik på udvikling og prøvning af visse innovative AI-systemer i sandkassen på følgende betingelser:
  - (a) de innovative AI-systemer skal udvikles med henblik på at beskytte væsentlige samfundsinteresser på et eller flere af følgende områder:
    - i) forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed, under de kompetente myndigheders kontrol og ansvar. Behandlingen skal være baseret på den pågældende medlemsstats lovgivning eller EU-retten
    - ii) den offentlige sikkerhed og folkesundheden, herunder sygdomsforebyggelse, -bekæmpelse og -behandling
    - iii) et højt niveau af miljøbeskyttelse og forbedring af miljøkvaliteten
  - (b) de behandlede oplysninger skal være nødvendige for at opfylde et eller flere af de krav, der er omhandlet i afsnit III, kapitel 2, såfremt disse krav ikke praktisk kan opfyldes ved behandling af anonymiserede eller syntetiske oplysninger eller andre oplysninger end personoplysninger
  - (c) der skal foreligge effektive overvågningsmekanismer til at konstatere, om der kan opstå store risici for de registreredes grundlæggende rettigheder i forbindelse med forsøgene i sandkassen, samt beredskabsmekanismer til straks at afbøde disse risici og om nødvendigt standse behandlingen
  - (d) alle personoplysninger, der skal behandles i forbindelse med sandkassen, skal befinde sig i et funktionelt adskilt, isoleret og beskyttet databehandlingsmiljø under deltagernes kontrol, og kun autoriserede personer har adgang til disse data
  - (e) de behandlede personoplysninger må ikke videregives, overføres eller på anden måde tilgås af andre parter
  - (f) enhver behandling af personoplysninger i forbindelse med sandkassen må ikke føre til foranstaltninger eller beslutninger, der berører de registrerede
  - (g) alle personoplysninger, der skal behandles i forbindelse med sandkassen, skal slettes, når deltagelsen i sandboksen afsluttes, eller når opbevaringsperioden for personoplysningerne udløber
  - (h) logfilerne over behandlingen af personoplysninger i forbindelse med sandkassen opbevares under deltagelsen i sandkassen og 1 år efter dens ophør udelukkende med henblik på og kun så længe, det er nødvendigt for at opfylde ansvarligheds- og dokumentationsforpligtelserne i henhold til denne artikel eller anden gældende EU-lovgivning eller national lovgivning
  - (i) der skal som en del af den tekniske dokumentation i bilag IV opbevares en fuldstændig og detaljeret beskrivelse af processen og begrundelsen for træningen, prøvningen og valideringen af AI-systemet sammen med prøvningsresultaterne

- (j) der skal på de kompetente myndigheders websted offentliggøres et kort resumé af det AI-projekt, der er udviklet i sandkassen, dets mål og dets forventede resultater.
2. Stk. 1 berører ikke Unionens eller medlemsstaternes lovgivning, der udelukker behandling til andre formål end dem, der udtrykkeligt er nævnt i den pågældende lovgivning.

#### *Artikel 55*

#### *Foranstaltninger for mindre udbydere og brugere*

1. Medlemsstaterne skal træffe følgende foranstaltninger:
- (a) give mindre udbydere og nystartede virksomheder prioriteret adgang til de reguleringsmæssige sandkasser for kunstig intelligens, i det omfang de opfylder betingelserne for deltagelse deri
  - (b) organisere specifikke oplysningsaktiviteter, der er tilpasset mindre udbyderes og brugeres behov, om anvendelsen af denne forordning
  - (c) etablere en særlig kommunikationskanal med mindre udbydere og brugere og andre innovatorer, hvor det er relevant, for at yde vejledning og besvare spørgsmål om gennemførelsen af denne forordning.
2. Der skal tages hensyn til de mindre udbyderes særlige interesser og behov ved fastsættelsen af gebyrerne for overensstemmelsesvurdering i henhold til artikel 43, idet gebyrerne nedsættes i forhold til deres størrelse og markedsstørrelse.

### **AFSNIT VI**

## **FORVALTNING**

### **KAPITEL 1**

## **DET EUROPÆISKE UDVALG FOR KUNSTIG INTELLIGENS**

#### *Artikel 56*

#### *Oprettelse af Det Europæiske Udvalg for Kunstig Intelligens*

1. Der oprettes et "Europæisk Udvalg for Kunstig Intelligens" ("udvalget").
2. Udvalget yder rådgivning og bistand til Kommissionen med henblik på at:
- (a) bidrage til et effektivt samarbejde mellem de nationale tilsynsmyndigheder og Kommissionen om anliggender, der er omfattet af denne forordning
  - (b) koordinere og bidrage til Kommissionens, de nationale tilsynsmyndigheders og andre kompetente myndigheders vejledning og analyser vedrørende nye spørgsmål i hele det indre marked med hensyn til anliggender, der er omfattet af denne forordning
  - (c) bistå de nationale tilsynsmyndigheder og Kommissionen med at sikre en ensartet anvendelse af denne forordning.

*Artikel 57*  
*Udvalgets struktur*

1. Udvalget består af de nationale tilsynsmyndigheder, der repræsenteres af lederen eller en tilsvarende embedsmand på højt plan i den pågældende myndighed, og Den Europæiske Tilsynsførende for Databeskyttelse. Andre nationale myndigheder kan indbydes til møderne, hvis de drøftede spørgsmål er relevante for dem.
2. Udvalget vedtager sin forretningsorden med simpelt flertal blandt medlemmerne med Kommissionens samtykke. Forretningsordenen skal også indeholde de operationelle aspekter i forbindelse med udførelsen af udvalgets opgaver som anført i artikel 58. Udvalget kan efter behov nedsætte undergrupper med henblik på at behandle specifikke spørgsmål.
3. Udvalgets formandskab varetages af Kommissionen. Kommissionen indkalder til møderne og udarbejder dagsordenen i overensstemmelse med udvalgets opgaver i henhold til denne forordning og dens forretningsorden. Kommissionen yder administrativ og analytisk støtte til Udvalgets aktiviteter i henhold til denne forordning.
4. Udvalget kan indbyde eksterne eksperter og observatører til at deltage i møderne og kan udveksle synspunkter med interesserede tredjeparter for at oplyse om sine aktiviteter i et passende omfang. Med henblik herpå kan Kommissionen lette udvekslingen mellem udvalget og andre af Unionens organer, kontorer, agenturer og rådgivende grupper.

*Artikel 58*  
*Udvalgets opgaver*

Når Udvalget yder rådgivning og bistand til Kommissionen i forbindelse med artikel 56, stk. 2, skal det navnlig:

- (a) indsamle og udveksle ekspertise og bedste praksis blandt medlemsstaterne
- (b) bidrage til en ensartet administrativ praksis i medlemsstaterne, herunder til driften af reguleringsmæssige sandkasser, jf. artikel 53
- (c) afgive udtalelser, henstillinger eller skriftlige bidrag om spørgsmål vedrørende gennemførelsen af denne forordning, navnlig
  - i) om tekniske specifikationer eller eksisterende standarder vedrørende de i afsnit III, kapitel 2, fastsatte krav
  - ii) om anvendelsen af harmoniserede standarder eller fælles specifikationer som omhandlet i artikel 40 og 41
  - iii) om udarbejdelse af vejledende dokumenter, herunder retningslinjerne for fastsættelse af administrative bøder, jf. artikel 71.

## KAPITEL 2

### NATIONALE KOMPETENTE MYNDIGHEDER

#### *Artikel 59*

#### *Udpegelse af nationale kompetente myndigheder*

1. Hver medlemsstat skal oprette eller udpege nationale kompetente myndigheder med henblik på at sikre denne forordnings anvendelse og gennemførelse. De nationale kompetente myndigheder skal være organiseret på en sådan måde, at der i deres arbejde og opgaver sikres objektivitet og uvildighed.
2. Hver medlemsstat skal udpege en national tilsynsmyndighed blandt de nationale kompetente myndigheder. Den nationale tilsynsmyndighed skal fungere som bemyndigende myndighed og markedsovervågningsmyndighed, medmindre en medlemsstat har organisatoriske og administrative grunde til at udpege mere end én myndighed.
3. Medlemsstaterne skal underrette Kommissionen om deres udpegelse(r) og, hvor det er relevant, om begrundelsen for at udpege mere end én myndighed.
4. Medlemsstaterne skal sikre, at de nationale kompetente myndigheder modtager tilstrækkelige finansielle og menneskelige ressourcer til at udføre deres opgaver i henhold til denne forordning. De nationale kompetente myndigheder skal navnlig råde over et tilstrækkeligt antal medarbejdere på fast basis, hvis kompetencer og ekspertise skal omfatte en indgående forståelse af AI-teknologier, data og databehandling, grundlæggende rettigheder og sundheds- og sikkerhedsrisici samt viden om gældende standarder og retlige krav.
5. Medlemsstaterne skal hvert år aflægge rapport til Kommissionen om status for de nationale kompetente myndigheders finansielle og menneskelige ressourcer med en vurdering af deres tilstrækkelighed. Kommissionen videresender disse oplysninger til udvalget med henblik på drøftelse og eventuelle henstillinger.
6. Kommissionen letter udvekslingen af erfaringer mellem de nationale kompetente myndigheder.
7. De nationale kompetente myndigheder kan yde vejledning og rådgivning om gennemførelsen af denne forordning, herunder til mindre udbydere. Når de nationale kompetente myndigheder agter at yde vejledning og rådgivning i forbindelse med et AI-system på områder, der er omfattet af anden EU-lovgivning, skal de kompetente nationale myndigheder høres i henhold til denne EU-lovgivning, hvis det er relevant. Medlemsstaterne kan også oprette et centralt kontaktpunkt til kommunikation med operatører.
8. I tilfælde hvor Unionens institutioner, agenturer og organer er omfattet af denne forordning, fungerer Den Europæiske Tilsynsførende for Databeskyttelse som den kompetente myndighed for tilsynet med dem.

## AFSNIT VII

### EU-DATABASE FOR SELVSTÆNDIGE HØJRISIKO-AI-SYSTEMER

#### *Artikel 60*

##### *EU-database for selvstændige højrisiko-AI-systemer*

1. Kommissionen opretter og vedligeholder i samarbejde med medlemsstaterne en EU-database med de i stk. 2 omhandlede oplysninger vedrørende højrisiko-AI-systemer, jf. artikel 6, stk. 2, som er registreret i overensstemmelse med artikel 51.
2. Udbyderne skal registrere de oplysninger, der er anført i bilag VIII, i EU-databasen. Kommissionen yder dem teknisk og administrativ støtte.
3. Oplysningerne i EU-databasen skal være offentligt tilgængelige.
4. EU-databasen må kun indeholde personoplysninger i det omfang, det er nødvendigt for at indsamle og behandle oplysninger i overensstemmelse med denne forordning. Disse oplysninger omfatter navne og kontaktoplysninger på de fysiske personer, der er ansvarlige for registrering af systemet og har retlig beføjelse til at repræsentere udbyderen.
5. Kommissionen er dataansvarlig for EU-databasen. Den sikrer også, at udbyderne modtager tilstrækkelig teknisk og administrativ støtte.

## AFSNIT VIII

### OVERVÅGNING EFTER OMSÆTNINGEN, UDVEKSLING AF OPLYSNINGER OG MARKEDSOVERVÅGNING

#### KAPITEL 1

##### OVERVÅGNING EFTER OMSÆTNINGEN

#### *Artikel 61*

##### *Udbydernes overvågning efter omsætningen og planer for overvågning efter omsætningen af højrisiko-AI-systemer*

1. Udbyderne skal oprette og dokumentere et system til overvågning efter omsætningen på en måde, der står i et rimeligt forhold til AI-teknologiernes art og risiciene ved højrisiko-AI-systemet.
2. Systemet til overvågning efter omsætningen skal aktivt og systematisk indsamle, dokumentere og analysere relevante data, som brugerne afgiver, eller som indsamles gennem andre kilder, om højrisiko-AI-systemers ydeevne i hele deres levetid og give udbyderen mulighed for at evaluere AI-systemernes fortsatte overholdelse de i afsnit III, kapitel 2, fastsatte krav.
3. Systemet til overvågning efter omsætningen skal baseres på en plan for overvågning efter omsætningen. Planen for overvågning efter omsætningen skal være en del af den tekniske dokumentation, jf. bilag IV. Kommissionen vedtager en gennemførelsesretsakt om detaljerede bestemmelser om en model for planen for overvågning efter omsætningen og listen over elementer, der skal indgå i planen.

4. For højrisiko-AI-systemer, der er omfattet af de retsakter, der er omhandlet i bilag II, hvor der allerede er etableret et system og en plan for overvågning efter omsætningen i henhold til denne lovgivning, skal de elementer, der er beskrevet i stk. 1, 2 og 3, integreres i systemet og planen, hvor det er relevant.

Første afsnit finder også anvendelse på de i bilag III, punkt 5, litra b), omhandlede højrisiko-AI-systemer, der bringes i omsætning eller tages i brug af kreditinstitutter, der er reguleret ved direktiv 2013/36/EU.

## KAPITEL 2

### UDVEKSLING AF OPLYSNINGER OM HÆNDELSER OG FUNKTIONSFEJL

#### *Artikel 62*

#### *Indberetning af alvorlige hændelser og funktionsfejl*

1. Udbydere af højrisiko-AI-systemer, der bringes i omsætning på EU-markedet, skal indberette enhver alvorlig hændelse eller funktionsfejl i forbindelse med disse systemer, som udgør en misligholdelse af forpligtelser i henhold til den del af EU-retten, der har til formål at beskytte de grundlæggende rettigheder, til markedsovervågningsmyndighederne i de medlemsstater, hvor hændelsen eller misligholdelsen fandt sted.

En sådan indberetning skal foretages umiddelbart efter, at udbyderen har fastslået en årsagssammenhæng mellem AI-systemet og hændelsen eller funktionsfejlen eller rimelig sandsynlighed for en sådan sammenhæng, og under alle omstændigheder senest 15 dage efter, at udbyderne har fået kendskab til den alvorlige hændelse eller funktionsfejlen.

2. Når markedsovervågningsmyndigheden modtager en indberetning vedrørende misligholdelse af forpligtelser i henhold til den del af EU-retten, der har til formål at beskytte de grundlæggende rettigheder, skal den underrette de nationale offentlige myndigheder eller organer, der er omhandlet i artikel 64, stk. 3. Kommissionen udarbejder særlig vejledning for at lette overholdelsen af forpligtelserne i stk. 1. Denne vejledning udstedes senest 12 måneder efter denne forordnings ikrafttræden.
3. I forbindelse med de i bilag III, punkt 5, litra b), omhandlede højrisiko-AI-systemer, der bringes i omsætning eller tages i brug af kreditinstitutter, der er reguleret ved direktiv 2013/36/EU, og for højrisiko-AI-systemer, der er beregnet til at blive anvendt som sikkerhedskomponenter i udstyr, eller som i selv er udstyr, der er omfattet af forordning (EU) 2017/745 og forordning (EU) 2017/746, begrænses indberetningen af alvorlige hændelser eller funktionsfejl til dem, der udgør en misligholdelse af forpligtelser i henhold til den del af EU-retten, der har til formål at beskytte de grundlæggende rettigheder.



## KAPITEL 3

### HÅNDHÆVELSE

#### *Artikel 63*

#### *Markedsovervågning og kontrol af AI-systemer på EU-markedet*

1. Forordning (EU) 2019/1020 finder anvendelse på AI-systemer, der er omfattet af nærværende forordning. Med henblik på effektiv håndhævelse af nærværende forordning gælder dog følgende:
  - (a) enhver henvisning til en erhvervsdrivende i henhold til forordning (EU) 2019/1020 skal forstås således, at den omfatter alle operatører, der er omfattet af afsnit III, kapitel 3, i nærværende forordning
  - (b) enhver henvisning til et produkt i henhold til forordning (EU) 2019/1020 skal forstås således, at den omfatter alle AI-systemer, der henhører under nærværende forordnings anvendelsesområde.
2. Den nationale tilsynsmyndighed skal regelmæssigt aflægge rapport til Kommissionen om resultaterne af relevante markedsovervågningsaktiviteter. Den nationale tilsynsmyndighed skal straks indberette alle oplysninger, der er fremskaffet i forbindelse med markedsovervågningsaktiviteter, og som kan være af potentiel interesse for anvendelsen af EU-lovgivningen om konkurrenceregler, til Kommissionen og de relevante nationale konkurrencemyndigheder.
3. For så vidt angår højrisiko-AI-systemer, som er knyttet til produkter, der er omfattet af de i bilag II, afsnit A, opførte retsakter, er markedsovervågningsmyndigheden med henblik på denne forordning den myndighed, der i henhold til disse retsakter er ansvarlig for markedsovervågningsaktiviteter.
4. For så vidt angår AI-systemer, der bringes i omsætning, tages i brug eller anvendes af finansielle institutioner, der er omfattet af EU-lovgivningen om finansielle tjenesteydelser, er markedsovervågningsmyndigheden med henblik på denne forordning den relevante myndighed, der i henhold til denne lovgivning er ansvarlig for det finansielle tilsyn med disse institutioner.
5. For så vidt angår AI-systemer, der er anført i punkt 1, litra a), i det omfang systemerne anvendes til retshåndhævelsesformål, jf. punkt 6 og 7 i bilag III, skal medlemsstaterne med henblik på denne forordning udpege som markedsovervågningsmyndigheder enten de kompetente datatilsynsmyndigheder i henhold til direktiv (EU) 2016/680 eller forordning 2016/679 eller de nationale kompetente myndigheder, der fører tilsyn med de retshåndhævelses-, indvandrings- eller asylmyndigheder, der ibrugtager eller anvender disse systemer.
6. I tilfælde hvor Unionens institutioner, agenturer og organer er omfattet af denne forordning, fungerer Den Europæiske Tilsynsførende for Databeskyttelse som deres markedsovervågningsmyndighed.
7. Medlemsstaterne skal fremme koordineringen mellem markedsovervågningsmyndigheder, der er udpeget i henhold til denne forordning, og andre relevante nationale myndigheder eller organer, der fører tilsyn med anvendelsen af den EU-harmoniseringslovgivning, der er opført i bilag II, eller anden EU-lovgivning, der kan være relevant for de i bilag III omhandlede højrisiko-AI-systemer.

*Artikel 64*  
*Adgang til oplysninger og dokumentation*

1. I forbindelse med deres arbejde skal markedsovervågningsmyndighederne have fuld adgang til de trænings-, validerings- og prøvningsdatasæt, der anvendes af udbyderen, herunder via programmeringsgrænseflader for applikationer ("API'er") eller andre passende tekniske midler og værktøjer, der muliggør fjernadgang.
2. Hvis det er nødvendigt for at vurdere, om højrisiko-AI-systemet er i overensstemmelse med kravene i afsnit III, kapitel 2, skal markedsovervågningsmyndighederne efter begrundet anmodning gives adgang til kildekoden for AI-systemet.
3. Nationale offentlige myndigheder eller organer, der fører tilsyn med eller håndhæver opfyldelsen af forpligtelser i henhold til EU-retten om beskyttelse af de grundlæggende rettigheder i forbindelse med anvendelsen af højrisiko-AI-systemer, jf. bilag III, har beføjelse til at anmode om og få adgang til al dokumentation, der er udarbejdet eller opretholdt i henhold til denne forordning, hvis adgang til denne dokumentation er nødvendig for udøvelsen af de beføjelser, der er omfattet af deres mandat, inden for rammerne af deres jurisdiktion. Den relevante offentlige myndighed eller det relevante offentlige organ skal underrette markedsovervågningsmyndigheden i den pågældende medlemsstat om enhver sådan anmodning.
4. Senest 3 måneder efter denne forordnings ikrafttræden skal hver medlemsstat identificere de offentlige myndigheder eller organer, der er omhandlet i stk. 3, og offentliggøre en liste på den nationale tilsynsmyndigheds websted. Medlemsstaterne skal sende listen til Kommissionen og alle de øvrige medlemsstater og holde listen ajour.
5. Hvis den i stk. 3 omhandlede dokumentation er utilstrækkelig til at fastslå, om der er sket en misligholdelse af forpligtelser i henhold til den del af EU-retten, der har til formål at beskytte de grundlæggende rettigheder, kan den offentlige myndighed eller det offentlige organ, der er omhandlet i stk. 3, fremsætte en begrundet anmodning til markedsovervågningsmyndigheden om at tilrettelægge prøvning af højrisiko-AI-systemet ved hjælp af tekniske midler. Markedsovervågningsmyndigheden skal tilrettelægge prøvningen med tæt inddragelse af den anmodende offentlige myndighed eller det anmodende offentlige organ inden for rimelig tid efter anmodningen.
6. Alle oplysninger og al dokumentation, som de i stk. 3 omhandlede nationale offentlige myndigheder eller organer modtager i henhold til bestemmelserne i denne artikel, skal behandles i overensstemmelse med tavshedspligten, jf. artikel 70.

*Artikel 65*  
*Procedure i tilfælde af AI-systemer, der udgør en risiko på nationalt plan*

1. AI-systemer, der udgør en risiko, skal forstås som et produkt, der udgør en risiko, som defineret i artikel 3, nr. 19), i forordning (EU) 2019/1020, for så vidt angår risici for menneskers sundhed eller sikkerhed eller for beskyttelsen af personers grundlæggende rettigheder.
2. Hvis en medlemsstats markedsovervågningsmyndighed har tilstrækkelig grund til at antage, at et AI-system udgør en risiko som omhandlet i stk. 1, skal den foretage en evaluering af det pågældende AI-system for så vidt angår dets opfyldelse af alle de

krav og forpligtelser, der er fastsat i denne forordning. Hvis der foreligger risici for beskyttelsen af de grundlæggende rettigheder, skal markedsovervågningsmyndigheden også underrette de relevante nationale offentlige myndigheder eller organer, der er omhandlet i artikel 64, stk. 3. De relevante operatører skal om nødvendigt samarbejde med markedsovervågningsmyndighederne og de andre nationale offentlige myndigheder eller organer, der er omhandlet i artikel 64, stk. 3.

Hvis markedsovervågningsmyndigheden i forbindelse med evalueringen konstaterer, at AI-systemet ikke opfylder kravene og forpligtelserne i denne forordning, skal de straks anmode den pågældende operatør om at træffe alle fornødne foranstaltninger for at sørge for, at AI-systemet opfylder kravene og forpligtelserne, trække AI-systemet tilbage fra markedet eller tilbagekalde det inden for en rimelig tidsfrist, som de fastsætter i forhold til risikoens art.

Markedsovervågningsmyndigheden skal underrette det relevante bemyndigede organ herom. Artikel 18 i forordning (EU) 2019/1020 finder anvendelse på de i andet afsnit omhandlede foranstaltninger.

3. Hvis markedsovervågningsmyndigheden konstaterer, at den manglende opfyldelse af kravene ikke er begrænset til medlemsstatens område, skal den underrette Kommissionen og de øvrige medlemsstater om resultaterne af evalueringen og om de tiltag, den har pålagt operatøren at iværksætte.
4. Operatøren skal sikre, at der træffes alle fornødne korrigerende foranstaltninger over for alle de pågældende AI-systemer, som denne har gjort tilgængelige på markedet i hele Unionen.
5. Hvis AI-systemets operatør ikke træffer de fornødne foranstaltninger inden for den frist, der er omhandlet i stk. 2, skal markedsovervågningsmyndigheden træffe de nødvendige foreløbige foranstaltninger for at forbyde eller begrænse AI-systemets tilgængelighed på deres nationale markeder eller for at trække produktet tilbage fra markedet eller kalde det tilbage. Den myndighed skal straks underrette Kommissionen og de øvrige medlemsstater om sådanne foranstaltninger.
6. De i stk. 5 omhandlede oplysninger skal indeholde alle tilgængelige oplysninger, særlig de nødvendige data til identifikation af det AI-system, der ikke opfylder kravene, AI-systemets oprindelse, arten af den påståede manglende opfyldelse af kravene og af den pågældende risiko, arten og varigheden af de trufne nationale foranstaltninger samt de synspunkter, som den pågældende operatør har fremsat. Markedsovervågningsmyndighederne skal navnlig oplyse, om den manglende overensstemmelse med kravene skyldes et eller flere af følgende:
  - (a) AI-systemets manglende opfyldelse af kravene i afsnit III, kapitel 2
  - (b) mangler ved de harmoniserede standarder eller fælles specifikationer, der er omhandlet i artikel 40 og 41, og som danner grundlag for overensstemmelsesformodningen.
7. Markedsovervågningsmyndighederne i de andre medlemsstater end markedsovervågningsmyndigheden i den medlemsstat, der har indledt proceduren, skal straks underrette Kommissionen og de øvrige medlemsstater om de trufne foranstaltninger og om yderligere oplysninger, som de måtte råde over, om det pågældende AI-systems manglende opfyldelse af kravene og om deres indsigelser, hvis de ikke er indforstået med den meddelte nationale foranstaltning.

8. Hvis der ikke inden for tre måneder efter modtagelsen af de i stk. 5 omhandlede oplysninger er blevet gjort indsigelse af en medlemsstat eller Kommissionen mod en foreløbig foranstaltning truffet af en medlemsstat, anses denne foranstaltning for at være berettiget. Dette berører ikke den pågældende operatørs procedurerettigheder i henhold til artikel 18 i forordning (EU) 2019/1020.
9. Markedsovervågningsmyndighederne i samtlige medlemsstater skal sikre, at der straks træffes de fornødne restriktive foranstaltninger med hensyn til det pågældende produkt, f.eks. tilbagetrækning af produktet fra deres marked.

#### *Artikel 66*

#### *Beskyttelsesprocedure på EU-plan*

1. Hvis en medlemsstat inden for tre måneder efter modtagelsen af den i artikel 65, stk. 5, omhandlede underretning har gjort indsigelse mod en foranstaltning truffet af en anden medlemsstat, eller hvis Kommissionen finder, at foranstaltningen er i strid med EU-retten, drøfter Kommissionen straks spørgsmålet med den relevante medlemsstat og den eller de relevante operatører og evaluerer den nationale foranstaltning. På grundlag af resultaterne af denne evaluering træffer Kommissionen senest 9 måneder efter den i artikel 65, stk. 5, omhandlede underretning afgørelse om, hvorvidt den nationale foranstaltning er berettiget eller ej, og meddeler den pågældende medlemsstat denne afgørelse.
2. Hvis den nationale foranstaltning anses for at være berettiget, skal samtlige medlemsstater træffe de nødvendige foranstaltninger for at sikre, at det AI-system, der ikke opfylder kravene, trækkes tilbage fra deres marked, og underrette Kommissionen herom. Hvis den nationale foranstaltning anses for ikke at være berettiget, skal den pågældende medlemsstat trække foranstaltningen tilbage.
3. Hvis den nationale foranstaltning anses for at være berettiget, og hvis AI-systemets manglende opfyldelse af kravene tilskrives mangler ved de harmoniserede standarder eller fælles specifikationer som omhandlet i denne forordnings artikel 40 og 41, anvender Kommissionen proceduren i artikel 11 i forordning (EU) nr. 1025/2012.

#### *Artikel 67*

#### *AI-systemer, som opfylder kravene, men som udgør en risiko*

1. Hvis en medlemsstats markedsovervågningsmyndighed efter at have foretaget en vurdering i henhold til artikel 65 finder, at et AI-system, selv om det opfylder kravene i denne forordning, udgør en risiko for menneskers sundhed eller sikkerhed, for misligholdelse af forpligtelser i henhold til den del af EU-retten, der har til formål at beskytte de grundlæggende rettigheder, eller for andre samfundsinteresser, skal den pålægge den pågældende operatør at træffe alle nødvendige foranstaltninger for at sikre, at det pågældende AI-system, når det bringes i omsætning eller tages i brug, ikke længere udgør en risiko, eller for at trække AI-systemet tilbage fra markedet eller kalde det tilbage inden for en rimelig tidsfrist, som den fastsætter i forhold til risikoens art.
2. Udbyderen eller andre relevante operatører skal sikre, at der træffes korrigerende foranstaltninger med hensyn til alle de pågældende AI-systemer, som de har gjort tilgængelige på markedet i hele Unionen, inden for den tidsfrist, der er fastsat af medlemsstatens markedsovervågningsmyndighed, jf. stk. 1.

3. Medlemsstaten skal straks underrette Kommissionen og de øvrige medlemsstater herom. Denne underretning skal indeholde alle tilgængelige oplysninger, især de nødvendige data til identifikation af de pågældende AI-systemer, AI-systemets oprindelse og forsyningskæde, arten af den pågældende risiko og arten og varigheden af de trufne nationale foranstaltninger.
4. Kommissionen drøfter straks spørgsmålet med medlemsstaterne og den pågældende operatør og vurderer de trufne nationale foranstaltninger. På grundlag af resultaterne af denne vurdering træffer Kommissionen afgørelse om, hvorvidt foranstaltningen er berettiget eller ej, og foreslår om nødvendigt passende foranstaltninger.
5. Kommissionen retter sin afgørelse til medlemsstaterne.

#### *Artikel 68*

#### *Formel manglende opfyldelse af kravene*

1. Hvis en medlemsstats markedsovervågningsmyndighed konstaterer et af følgende forhold, skal den pålægge den pågældende udbyder at bringe den manglende opfyldelse af kravene til ophør:
  - (a) overensstemmelsesmærkningen er anbragt i modstrid med artikel 49
  - (b) der er ikke anbragt nogen overensstemmelsesmærkning
  - (c) der er ikke udarbejdet en EU-overensstemmelseserklæring
  - (d) EU-overensstemmelseserklæringen er ikke udarbejdet korrekt
  - (e) der er ikke anbragt noget identifikationsnummer for det bemyndigede organ, der er involveret i overensstemmelsesvurderingsproceduren, hvor dette er relevant.
2. Hvis der fortsat er tale om manglende opfyldelse af kravene som omhandlet i stk. 1, skal den pågældende medlemsstat træffe alle nødvendige foranstaltninger for at begrænse eller forbyde, at AI-systemet gøres tilgængeligt på markedet, eller sikre, at det kaldes tilbage eller trækkes tilbage fra markedet.

### **AFSNIT IX**

### **ADFÆRDSKODEKSER**

#### *Artikel 69*

#### *Adfærdskodekser*

1. Kommissionen og medlemsstaterne tilskynder til og letter udarbejdelsen af adfærdskodekser, der har til formål at fremme frivillig anvendelse af de i afsnit III, kapitel 2, fastsatte krav på AI-systemer, der ikke er højrisiko-AI-systemer, på grundlag af tekniske specifikationer og løsninger, der er egnede til at sikre opfyldelsen af disse krav i lyset af systemernes tilsigtede formål.
2. Kommissionen og udvalget tilskynder til og letter udarbejdelsen af adfærdskodekser, der har til formål at fremme frivillig anvendelse af krav vedrørende f.eks. miljømæssig bæredygtighed, tilgængelighed for personer med handicap, interessenters deltagelse i udformningen og udviklingen af AI-systemerne og mangfoldighed blandt udviklingsteams på grundlag af klare mål og centrale resultatindikatorer til måling af realiseringen af disse mål.

3. Adfærdskodekser kan udarbejdes af individuelle udbydere af AI-systemer, af organisationer, der repræsenterer dem, eller af begge, herunder med inddragelse af brugere og eventuelle interesserede parter og deres repræsentative organisationer. Adfærdskodekser kan omfatte et eller flere AI-systemer under hensyntagen til ligheden mellem de relevante systemers tilsigtede formål.
4. Når Kommissionen og udvalget tilskynder til og letter udarbejdelsen af adfærdskodekser, tager de hensyn til de mindre udbyderes og nystartede virksomheders særlige interesser og behov.

## AFSNIT X

### TAVSHEDSPLIGT OG SANKTIONER

#### *Artikel 70 Tavshedspligt*

1. De nationale kompetente myndigheder og bemyndigede organer, der er involveret i anvendelsen af denne forordning, skal overholde tavshedspligten for oplysninger og data, der indhentes under udførelsen af deres opgaver og arbejde, på en sådan måde, at de navnlig beskytter:
  - (a) intellektuelle ejendomsrettigheder og fysiske eller juridiske personers fortrolige forretningsoplysninger eller forretningshemmeligheder, herunder kildekode, med undtagelse af de tilfælde, der er omhandlet i artikel 5 i direktiv 2016/943 om beskyttelse af fortrolig knowhow og fortrolige forretningsoplysninger (forretningshemmeligheder) mod ulovlig erhvervelse, brug og videregivelse
  - (b) den effektive gennemførelse af denne forordning, navnlig for så vidt angår inspektioner, undersøgelser eller audit) offentlige og nationale sikkerhedsinteresser
  - (c) strafferetlige eller administrative procedurers integritet.
2. Uden at berører stk. 1, må oplysninger, der udveksles fortroligt mellem de nationale kompetente myndigheder og mellem de nationale kompetente myndigheder og Kommissionen, ikke videregives uden forudgående høring af den oprindelige nationale kompetente myndighed og brugeren, i tilfælde hvor højrisiko-AI-systemer som omhandlet i bilag III, punkt 1, 6 og 7, anvendes af retshåndhævende myndigheder, indvandringsmyndigheder eller asylmyndigheder, hvis en sådan videregivelse ville bringe offentlige og nationale sikkerhedsinteresser i fare.

I tilfælde hvor de retshåndhævende myndigheder, indvandringsmyndighederne eller asylmyndighederne er udbydere af højrisiko-AI-systemer, jf. bilag III, punkt 1, 6 og 7, skal den tekniske dokumentation, der er omhandlet i bilag IV, forblive hos disse myndigheder. Disse myndigheder skal sikre, at de markedsovervågningsmyndigheder, der er omhandlet i artikel 63, stk. 5 og 6, alt efter hvad der er relevant, efter anmodning straks kan få adgang til dokumentationen eller få en kopi heraf. Kun det af markedsovervågningsmyndighedens personale, der har et passende sikkerhedsgodkendelsesniveau, må få adgang til dokumentationen eller en kopi heraf.
3. Stk. 1 og 2 berører ikke Kommissionens, medlemsstaternes og de bemyndigede organers rettigheder og forpligtelser med hensyn til udveksling af oplysninger og

udsendelse af advarsler eller de berørte parter forpligtelse til at afgive oplysninger inden for rammerne af medlemsstaternes straffelovgivning.

4. Kommissionen og medlemsstaterne kan om nødvendigt udveksle fortrolige oplysninger med reguleringsmyndigheder i tredjelande, med hvilke de har indgået bilaterale eller multilaterale aftaler om fortrolighed, der garanterer en tilstrækkelig grad af fortrolighed.

#### *Artikel 71* *Sanktioner*

1. I overensstemmelse med de vilkår og betingelser, der er fastsat i denne forordning, skal medlemsstaterne fastsætte regler om sanktioner, herunder administrative bøder, for overtrædelse af denne forordning og træffe alle nødvendige foranstaltninger for at sikre, at de gennemføres korrekt og effektivt. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning. Der skal navnlig tages hensyn til mindre udbyderes og nystartede virksomheders interesser og deres økonomiske levedygtighed.
2. Medlemsstaterne skal give Kommissionen meddelelse om disse regler og foranstaltninger og skal straks underrette den om senere ændringer, der berører dem.
3. Følgende overtrædelser skal straffes med administrative bøder på op til 30 000 000 EUR eller, hvis gerningsmanden er en virksomhed, op til 6 % af dens samlede globale årsomsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst:
  - (a) manglende overholdelse af forbuddet mod de i artikel 5 anførte former for praksis med hensyn til kunstig intelligens
  - (b) AI-systemets manglende opfyldelse af kravene i artikel 10.
4. AI-systemets manglende opfyldelse af ethvert krav eller enhver forpligtelse i henhold til denne forordning, bortset fra kravene i artikel 5 og 10, skal straffes med administrative bøder på op til 20 000 000 EUR eller, hvis lovovertræderen er en virksomhed, op til 4 % af dens samlede globale årlige omsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst.
5. Afgivelse af ukorrekte, ufuldstændige eller vildledende oplysninger til bemyndigede organer og nationale kompetente myndigheder som svar på en anmodning skal straffes med administrative bøder på op til 10 000 000 EUR eller, hvis lovovertræderen er en virksomhed, op til 2 % af dens samlede globale årlige omsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst.
6. Ved fastsættelsen af den administrative bødes størrelse skal der i hvert enkelt tilfælde tages hensyn til alle relevante omstændigheder i den specifikke situation, og der skal tages behørigt hensyn til følgende:
  - (a) overtrædelsens art, grovhed og varighed samt dens konsekvenser
  - (b) hvorvidt andre markedsovervågningsmyndigheder allerede har pålagt den samme operatør administrative bøder for samme overtrædelse
  - (c) størrelsen på den operatør, der har begået overtrædelsen, og dens markedsandel.

7. Hver medlemsstat skal fastsætte regler om, hvorvidt og i hvilket omfang administrative bøder må pålægges offentlige myndigheder og organer, der er etableret i den pågældende medlemsstat.
8. Afhængigt af medlemsstaternes retssystem kan reglerne om administrative bøder anvendes på en sådan måde, at bøderne pålægges af kompetente nationale domstole eller andre organer, alt efter hvad der er relevant i disse medlemsstater. Anvendelsen af disse regler i disse medlemsstater har tilsvarende virkning.

#### *Artikel 72*

##### *Administrative bøder til Unionens institutioner, agenturer og organer*

1. Den Europæiske Tilsynsførende for Databeskyttelse kan pålægge de af Unionens institutioner, agenturer og organer, der er omfattet af denne forordnings anvendelsesområde, administrative bøder. Når der træffes afgørelse om, hvorvidt der skal pålægges en administrativ bøde, og ved fastsættelsen af den administrative bødes størrelse skal der i hvert enkelt tilfælde tages hensyn til alle relevante omstændigheder i den specifikke situation, og der skal tages behørigt hensyn til følgende:
  - (a) overtrædelsens art, grovhed og varighed samt dens konsekvenser
  - (b) samarbejdet med Den Europæiske Tilsynsførende for Databeskyttelse med henblik på at afhjælpe overtrædelsen og afbøde de mulige negative virkninger af overtrædelsen, herunder overholdelse af enhver af de foranstaltninger, som Den Europæiske Tilsynsførende for Databeskyttelse tidligere har pålagt den eller det pågældende af Unionens institutioner, agenturer eller organer med hensyn til samme genstand
  - (c) eventuelle lignende overtrædelser, som den eller det pågældende af Unionens institutioner, agenturer eller organer tidligere har begået.
2. Der pålægges administrative bøder på op til 500 000 EUR for følgende overtrædelser:
  - (a) manglende overholdelse af forbuddet mod de i artikel 5 anførte former for praksis med hensyn til kunstig intelligens
  - (b) AI-systemets manglende opfyldelse af kravene i artikel 10.
3. AI-systemets manglende opfyldelse af ethvert krav eller enhver forpligtelse i henhold til denne forordning, bortset fra kravene i artikel 5 og 10, skal straffes med administrative bøder på op til 250 000 EUR.
4. Inden der træffes afgørelse i henhold til denne artikel, giver Den Europæiske Tilsynsførende for Databeskyttelse den eller det af Unionens institutioner, agenturer eller organer, der er genstand for de procedurer, som gennemføres af Den Europæiske Tilsynsførende for Databeskyttelse, muligheden for at blive hørt om genstanden for den mulige overtrædelse. Den Europæiske Tilsynsførende for Databeskyttelse baserer udelukkende sine afgørelser på elementer og forhold, som de berørte parter har haft mulighed for at fremsætte bemærkninger til. Eventuelle klager inddrages i vid udstrækning i proceduren.
5. De deltagende parter ret til forsvar skal sikres fuldt ud i procedureforløbet. De har ret til aktindsigt i Den Europæiske Tilsynsførende for Databeskyttelses sagsakter



med forbehold af fysiske personers eller virksomheders berettigede interesse i at beskytte deres personoplysninger eller forretningshemmeligheder.

6. Midler, der er indsamlet ved pålæg af bøder som omhandlet i denne artikel, tilfalder Unionens almindelige budget.

## **AFSNIT XI**

### **DELEGATION AF BEFØJELSER OG UDVALGSPROCEDURE**

#### *Artikel 73*

##### *Udøvelse af de delegerede beføjelser*

1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.
2. Den i artikel 4, artikel 7, stk. 1, artikel 11, stk. 3, artikel 43, stk. 5 og 6, og artikel 48, stk. 5, omhandlede delegation af beføjelser tillægges Kommissionen for en ubegrænset periode fra [datoen for denne forordnings ikrafttræden].
3. Den i artikel 4, artikel 7, stk. 1, artikel 11, stk. 3, artikel 43, stk. 5 og 6, og artikel 48, stk. 5, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i *Den Europæiske Unions Tidende* eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.
4. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.
5. Enhver delegeret retsakt vedtaget i henhold til artikel 4, artikel 7, stk. 1, artikel 11, stk. 3, artikel 43, stk. 5 og 6, og artikel 48, stk. 5, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på tre måneder fra underretningen om den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har informeret Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med tre måneder på Europa-Parlamentets eller Rådets initiativ.

#### *Artikel 74*

##### *Udvalgsprocedure*

1. Kommissionen bistås af et udvalg. Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011.
2. Når der henvises til dette stykke, finder artikel 5 i forordning (EU) nr. 182/2011 anvendelse.

## AFSNIT XII

### AFSLUTTENDE BESTEMMELSER

#### *Artikel 75*

##### *Ændring af forordning (EF) nr. 300/2008*

I artikel 4, stk. 3, i forordning (EF) nr. 300/2008, tilføjes følgende afsnit:

"Når der vedtages detaljerede foranstaltninger vedrørende tekniske specifikationer og procedurer for godkendelse og brug af sikkerhedsudstyr vedrørende systemer med kunstig intelligens, jf. definitionen i Europa-Parlamentets og Rådets forordning (EU) YYY/XX [om kunstig intelligens]\*, skal der tages hensyn til kravene i afsnit III, kapitel 2, i nævnte forordning."

---

\* Forordning (EU) YYY/XX [om kunstig intelligens] (EUT ...)."

#### *Artikel 76*

##### *Ændring af forordning (EU) nr. 167/2013*

I artikel 17, stk. 5, i forordning (EU) nr. 167/2013 tilføjes følgende afsnit:

"Når der i henhold til første afsnit vedtages delegerede retsakter vedrørende systemer med kunstig intelligens, som er sikkerhedskomponenter, jf. definitionen i Europa-Parlamentets og Rådets forordning (EU) YYY/XX [om kunstig intelligens]\*, skal der tages hensyn til kravene i afsnit III, kapitel 2, i nævnte forordning."

---

\* Forordning (EU) YYY/XX [om kunstig intelligens] (EUT ...)."

#### *Artikel 77*

##### *Ændring af forordning (EU) nr. 168/2013*

I artikel 22, stk. 5, i forordning (EU) nr. 168/2013 tilføjes følgende afsnit:

"Når der i henhold til første afsnit vedtages delegerede retsakter vedrørende systemer med kunstig intelligens, som er sikkerhedskomponenter, jf. definitionen i Europa-Parlamentets og Rådets forordning (EU) YYY/XX [om kunstig intelligens]\*, skal der tages hensyn til kravene i afsnit III, kapitel 2, i nævnte forordning."

---

\* Forordning (EU) YYY/XX [om kunstig intelligens] (EUT ...)."

#### *Artikel 78*

##### *Ændring af direktiv 2014/90/EU*

I artikel 8 i direktiv 2014/90/EU tilføjes følgende stykke:

"4. For så vidt angår systemer med kunstig intelligens, som er sikkerhedskomponenter, jf. definitionen i Europa-Parlamentets og Rådets forordning (EU) YYY/XX [om kunstig intelligens]\*, tager Kommissionen, når den udfører sine aktiviteter i henhold til stk. 1, og når

den vedtager tekniske specifikationer og prøvningsstandarder i overensstemmelse med stk. 2 og 3, hensyn til kravene i afsnit III, kapitel 2, i nævnte forordning.

---

\* Forordning (EU) YYY/XX [om kunstig intelligens] (EUT ...)."

*Artikel 79*  
*Ændring af direktiv (EU) 2016/797*

I artikel 5 i direktiv (EU) 2016/797 tilføjes følgende stykke:

"12. Når der i henhold til stk. 1 vedtages delegerede retsakter eller i henhold til stk. 11 vedtages gennemførelsesretsakter vedrørende systemer med kunstig intelligens, som er sikkerhedskomponenter, jf. definitionen i Europa-Parlamentets og Rådets forordning (EU) YYY/XX [om kunstig intelligens]\*, skal der tages hensyn til kravene i afsnit III, kapitel 2, i nævnte forordning.

---

\* Forordning (EU) YYY/XX [om kunstig intelligens] (EUT ...)."

*Artikel 80*  
*Ændring af forordning (EU) 2018/858*

I artikel 5 i forordning (EU) 2018/858 tilføjes følgende stykke:

"4. Når der i henhold til stk. 3 vedtages delegerede retsakter vedrørende systemer med kunstig intelligens, som er sikkerhedskomponenter, jf. definitionen i Europa-Parlamentets og Rådets forordning (EU) YYY/XX [om kunstig intelligens]\*, skal der tages hensyn til kravene i afsnit III, kapitel 2, i nævnte forordning.

---

\* Forordning (EU) YYY/XX [om kunstig intelligens] (EUT ...)."

*Artikel 81*  
*Ændring af forordning (EU) 2018/1139*

I forordning (EU) 2018/1139 foretages følgende ændringer:

1. I artikel 17 tilføjes følgende stykke:

"3. Uden at det berører stk. 2, når der i henhold til stk. 1 vedtages gennemførelsesretsakter vedrørende systemer med kunstig intelligens, som er sikkerhedskomponenter, jf. definitionen i Europa-Parlamentets og Rådets forordning (EU) YYY/XX [om kunstig intelligens]\*, skal der tages hensyn til kravene i afsnit III, kapitel 2, i nævnte forordning.

---

\* Forordning (EU) YYY/XX [om kunstig intelligens] (EUT ...)."

2. I artikel 19 tilføjes følgende stykke:

"4. Når der i henhold til stk. 1 og 2 vedtages delegerede retsakter vedrørende systemer med kunstig intelligens, som er sikkerhedskomponenter, jf. definitionen i forordning (EU) YYY/XX [om kunstig intelligens], skal der tages hensyn til kravene i afsnit III, kapitel 2, i nævnte forordning."

3. I artikel 43 tilføjes følgende stykke:

"4. Når der i henhold til stk. 1 vedtages gennemførelsesretsakter vedrørende systemer med kunstig intelligens, som er sikkerhedskomponenter, jf. definitionen i forordning (EU) YYY/XX [om kunstig intelligens], skal der tages hensyn til kravene i afsnit III, kapitel 2, i nævnte forordning."

4. I artikel 47 tilføjes følgende stykke:

"3. Når der i henhold til stk. 1 og 2 vedtages delegerede retsakter vedrørende systemer med kunstig intelligens, som er sikkerhedskomponenter, jf. definitionen i forordning (EU) YYY/XX [om kunstig intelligens], skal der tages hensyn til kravene i afsnit III, kapitel 2, i nævnte forordning."

5. I artikel 57 tilføjes følgende stykke:

"Når der vedtages sådanne gennemførelsesretsakter vedrørende systemer med kunstig intelligens, som er sikkerhedskomponenter, jf. definitionen i forordning (EU) YYY/XX [om kunstig intelligens], skal der tages hensyn til kravene i afsnit III, kapitel 2, i nævnte forordning."

6. I artikel 58 tilføjes følgende stykke:

"3. Når der i henhold til stk. 1 og 2 vedtages delegerede retsakter vedrørende systemer med kunstig intelligens, som er sikkerhedskomponenter, jf. definitionen i forordning (EU) YYY/XX [om kunstig intelligens], skal der tages hensyn til kravene i afsnit III, kapitel 2, i nævnte forordning."

#### *Artikel 82*

#### *Ændring af forordning (EU) 2019/2144*

I artikel 11 i forordning (EU) 2019/2144 tilføjes følgende stykke:

"3. "Når der i henhold til stk. 2 vedtages gennemførelsesretsakter vedrørende systemer med kunstig intelligens, som er sikkerhedskomponenter, jf. definitionen i Europa-Parlamentets og Rådets forordning (EU) YYY/XX [om kunstig intelligens]\*, skal der tages hensyn til kravene i afsnit III, kapitel 2, i nævnte forordning.

---

\* Forordning (EU) YYY/XX [om kunstig intelligens] (EUT ...)."

#### *Artikel 83*

#### *AI-systemer, der allerede er bragt i omsætning eller taget i brug*

1. Denne forordning finder ikke anvendelse på AI-systemer, som er komponenter i de store IT-systemer, der er oprettet ved de retsakter, der er opført i bilag IX, og som er blevet bragt i omsætning eller taget i brug før den [12 måneder efter datoen for denne forordnings anvendelse, jf. artikel 85, stk. 2], medmindre erstatning eller ændring af disse retsakter medfører en væsentlig ændring af det eller de pågældende AI-systemers design eller tilsigtede formål.

De krav, der er fastsat i denne forordning, skal, hvor det er relevant, tages i betragtning ved den evaluering, som skal foretages i henhold til de retsakter, der er opført i bilag IX, af hvert af de store IT-systemer, der er oprettet ved disse respektive retsakter.

2. Denne forordning finder kun anvendelse på andre højrisiko-AI-systemer end dem, der er omhandlet i stk. 1, og som er bragt i omsætning eller taget i brug inden den [datoen for denne forordnings anvendelse, jf. artikel 85, stk. 2], hvis disse systemer fra denne dato er genstand for betydelige ændringer af deres design eller tilsigtede formål.

*Artikel 84*  
*Evaluering og revision*

1. Kommissionen vurderer behovet for at ændre listen i bilag III en gang om året efter denne forordnings ikrafttræden.
2. Senest [tre år efter datoen for denne forordnings anvendelse, jf. artikel 85, stk. 2] og hvert fjerde år derefter forelægger Kommissionen Europa-Parlamentet og Rådet en rapport om evaluering og revision af denne forordning. Rapporterne offentliggøres.
3. I de i stk. 2 omhandlede rapporter lægges der særlig vægt på følgende:
  - (a) status over de nationale kompetente myndigheders finansielle og menneskelige ressourcer med henblik på effektivt at udføre de opgaver, de pålægges i henhold til denne forordning
  - (b) status over de sanktioner og navnlig de administrative bøder, der er omhandlet i artikel 71, stk. 1, som medlemsstaterne har pålagt som følge af overtrædelser af bestemmelserne i denne forordning.
4. Senest [tre år efter datoen for denne forordnings anvendelse, jf. artikel 85, stk. 2] og hvert fjerde år derefter evaluerer Kommissionen virkningen og effektiviteten af adfærdskodekser med henblik på at fremme anvendelsen af kravene i afsnit III, kapitel 2, og eventuelt andre yderligere krav til andre AI-systemer end højrisiko-AI-systemer.
5. Med henblik på stk. 1-4 indgiver udvalget, medlemsstaterne og de nationale kompetente myndigheder oplysninger til Kommissionen på dennes anmodning.
6. Når Kommissionen foretager evaluering og revision, jf. stk. 1-4, tager den hensyn til holdninger og resultater fra udvalget, fra Europa-Parlamentet, fra Rådet og fra andre relevante organer eller kilder.
7. Kommissionen forelægger om nødvendigt relevante forslag til ændring af denne forordning, navnlig under hensyntagen til den teknologiske udvikling og i lyset af fremskridtene i informationssamfundet.

*Artikel 85*  
*Ikrafttræden og anvendelse*

1. Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.
2. Denne forordning anvendes fra [24 måneder efter forordningens ikrafttræden].
3. Uanset stk. 2:
  - (a) anvendes afsnit III, kapitel 4, og afsnit VI fra den [tre måneder efter denne forordnings ikrafttræden]
  - (b) anvendes artikel 71 fra den [12 måneder efter denne forordnings ikrafttræden].

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.  
Udfærdiget i Bruxelles, den [...].

*På Europa-Parlamentets vegne*  
*Formand*

*På Rådets vegne*  
*Formand*

## **FINANSIERINGSOVERSIGT**

### **1. FORSLAGETS/INITIATIVETS RAMME**

- 1.1. Forslagets/initiativets betegnelse
- 1.2. Berørt(e) politikområde(r)
- 1.3. Forslaget/initiativet vedrører
- 1.4. Mål
  - 1.4.1. Generelt/generelle mål
  - 1.4.2. Specifikt/specifikke mål
  - 1.4.3. Forventet/forventede resultat(er) og virkning(er)
  - 1.4.4. Resultatindikatorer
- 1.5. Begrundelse for forslaget/initiativet
  - 1.5.1. Behov, der skal opfyldes på kort eller lang sigt, herunder en detaljeret tidsplan for iværksættelsen af initiativet
  - 1.5.2. Merværdien ved et EU-tiltag (f.eks. som følge af koordineringsfordele, retssikkerhed, større effekt eller komplementaritet). Ved "merværdien ved et EU-tiltag" forstås her merværdien af EU's intervention i forhold til den værdi, som medlemsstaterne ville have skabt enkeltvis
  - 1.5.3. Erfaringer fra tidligere foranstaltninger af lignende art
  - 1.5.4. Forenelighed med den flerårige finansielle ramme og mulige synergivirkninger med andre relevante instrumenter
  - 1.5.5. Vurdering af de forskellige finansieringsmuligheder, der er til rådighed, herunder muligheden for omfordeling
- 1.6. Forslagets/initiativets varighed og finansielle virkninger
- 1.7. Planlagt(e) forvaltningsmetode(r)

### **2. FORVALTNINGSFORANSTALTNINGER**

- 2.1. Bestemmelser om overvågning og rapportering
- 2.2. Forvaltnings- og kontrolsystem
  - 2.2.1. Begrundelse for den/de foreslåede forvaltningsmetode(r), finansieringsmekanisme(r), betalingsvilkår og kontrolstrategi
  - 2.2.2. Oplysninger om de konstaterede risici og det/de interne kontrolsystem(er), der etableres for at afbøde dem
  - 2.2.3. Vurdering af og begrundelse for kontrolforanstaltningernes omkostningseffektivitet (forholdet mellem kontrolomkostningerne og værdien af de forvaltede midler) samt vurdering af den forventede risiko for fejl (ved betaling og ved afslutning)

2.3. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

### **3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER**

3.1. Berørt(e) udgiftsområde(r) i den flerårige finansielle ramme og udgiftspost(er) på budgettet

3.2. Forslagets anslåede finansielle virkninger for bevillingerne

*3.2.1. Sammenfatning af de anslåede virkninger for aktionsbevillingerne*

*3.2.2. Anslåede resultater finansieret med aktionsbevillinger*

*3.2.3. Sammenfatning af de anslåede virkninger for administrationsbevillingerne*

*3.2.4. Forenelighed med indeværende flerårige finansielle ramme*

*3.2.5. Bidrag fra tredjemand*

3.3. Anslåede virkninger for indtægterne



## **FINANSIERINGSOVERSIGT**

### **1. FORSLAGETS/INITIATIVETS RAMME**

#### **1.1. Forslagets/initiativets betegnelse**

Europa-Parlamentets og Rådets forordning om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens) og om ændring af visse af Unionens lovgivningsmæssige retsakter

#### **1.2. Berørt(e) politikområde(r)**

Kommunikationsnet, Indhold og Teknologi

Det Indre Marked, Erhvervs politik, Iværksætteri og SMV'er

De budgetmæssige konsekvenser vedrører de nye opgaver, som Kommissionen har fået overdraget, herunder støtte til Det Europæiske Udvalg for Kunstig Intelligens

Aktivitet: Europas digitale fremtid i støbeskeen

#### **1.3. Forslaget/initiativet vedrører**

**en ny foranstaltning**

**en ny foranstaltning som opfølgning på et pilotprojekt/en forberedende foranstaltning<sup>64</sup>**

**en forlængelse af en eksisterende foranstaltning**

**omlægning af en foranstaltning til en ny foranstaltning**

#### **1.4. Mål**

##### *1.4.1. Generelt/generelle mål*

Det overordnede mål med tiltaget er at sikre et velfungerende indre marked ved at skabe gunstige betingelser for udvikling og anvendelse af pålidelig kunstig intelligens i Unionen.

##### *1.4.2. Specifikt/specifikke mål*

###### Specifikt mål nr. 1

At fastsætte krav, der er specifikke for AI-systemer, og forpligtelser for alle deltagere i værdikæden for at sikre, at AI-systemer, der bringes i omsætning og tages i brug, er sikre og overholder den gældende lovgivning om grundlæggende rettigheder og Unionens værdier

###### Specifikt mål nr. 2

At sikre retssikkerhed for at fremme investeringer og innovation inden for kunstig intelligens ved at gøre det klart, hvilke væsentlige krav, forpligtelser samt overensstemmelses- og overholdelsesprocedurer der skal følges for at bringe et AI-system i omsætning eller tage det i brug på EU-markedet

###### Specifikt mål nr. 3

<sup>64</sup> Jf. finansforordningens artikel 54, stk. 2, litra a) hhv. b).

At forbedre forvaltningen og den effektive håndhævelse af den eksisterende lovgivning om grundlæggende rettigheder og sikkerhedskrav, der gælder for AI-systemer, ved at give relevante myndigheder nye beføjelser og ressourcer samt klare regler om overensstemmelsesvurderingsprocedurer, efterfølgende overvågningsprocedurer og fordelingen af forvaltnings- og tilsynsopgaver på hhv. nationalt niveau og EU-plan

#### Specifikt mål nr. 4

At lette udviklingen af et indre marked for lovlige, sikre og pålidelige AI-anvendelser og forhindre markedsfragmentering ved at træffe EU-foranstaltninger for at fastsætte minimumskrav for AI-systemer, der skal bringes i omsætning og tages i brug på EU-markedet i overensstemmelse med gældende lovgivning om grundlæggende rettigheder og sikkerhed.

#### 1.4.3. *Forventet/forventede resultat(er) og virkning(er)*

*Angiv, hvilke virkninger forslaget/initiativet forventes at få for modtagerne/målgrupperne.*

Udbydere af kunstig intelligens bør nyde godt af et minimalt, men klart sæt krav, der skaber retssikkerhed og sikrer adgang til hele det indre marked.

Brugerne af AI-systemer bør have retssikkerhed for, at de AI-systemer, de køber, overholder europæiske love og værdier.

Forbrugerne bør nyde godt af en mindre risiko for trusler mod deres sikkerhed og krænkelse af deres grundlæggende rettigheder.

#### 1.4.4. *Resultatindikatorer*

*Angiv indikatorerne til kontrol af forslagets/initiativets gennemførelse.*

##### Indikator 1

Antal alvorlige hændelser eller handlinger udført af AI-systemer, som udgør alvorlige hændelser eller misligholdelse af forpligtelserne vedrørende de grundlæggende rettigheder, opgjort (halvårligt) efter anvendelsesområde og beregnet a) i absolutte tal, b) som andel pr. iværksat anvendelse og c) som andel pr. berørt borger.

##### Indikator 2

a) AI-investeringer i alt i EU (på årsbasis)

b) AI-investeringer i alt pr. medlemsstat (på årsbasis)

c) andel af virksomheder, der anvender kunstig intelligens (på årsbasis)

d) andel af SMV'er, der anvender kunstig intelligens (på årsbasis)

a) og b) beregnes på grundlag af officielle kilder og benchmarks i forhold til private overslag

c) og d) fastslås ved regelmæssige virksomhedsundersøgelser

## 1.5. Begrundelse for forslaget/initiativet

### 1.5.1. *Behov, der skal opfyldes på kort eller lang sigt, herunder en detaljeret tidsplan for iværksættelsen af initiativet*

Forordningen bør finde fuld anvendelse halvandet år efter vedtagelsen. Elementer i forvaltningsstrukturen bør dog være på plads inden da. Medlemsstaterne skal navnlig have udpeget eksisterende myndigheder og/eller oprettet nye myndigheder til at udføre de i den ovenstående lovgivning omhandlede opgaver, og Det Europæiske Udvalg for Kunstig Intelligens bør oprettes og være funktionsdygtigt. På det tidspunkt, hvor den europæiske database over AI-systemer finder anvendelse, bør databasen være fuldt ud funktionel. Parallelt med vedtagelsesprocessen er det derfor nødvendigt at udvikle databasen, således at dens udvikling er afsluttet, når forordningen træder i kraft.

### 1.5.2. *Merværdien ved et EU-tiltag (f.eks. som følge af koordineringsfordele, retssikkerhed, større effekt eller komplementaritet). Ved "merværdien ved et EU-tiltag" forstås her merværdien af EU's intervention i forhold til den værdi, som medlemsstaterne ville have skabt enkeltvis*

Et kludetæppe af potentielt divergerende nationale regler vil forhindre et gnidningsløst udbud af AI-systemer i hele EU og vil være ineffektivt med hensyn til at garantere sikkerheden, beskyttelsen af de grundlæggende rettigheder og Unionens værdier i de forskellige medlemsstater. En fælles EU-lovgivningsforanstaltning vedrørende kunstig intelligens kan sætte skub i det indre marked og har et stort potentiale til at give den europæiske industri både en konkurrencefordel på den globale scene og stordriftsfordele, som ikke kan opnås af de enkelte medlemsstater alene.

### 1.5.3. *Erfaringer fra tidligere foranstaltninger af lignende art*

Direktiv 2000/31/EF om elektronisk handel udgør den centrale ramme for det indre markeds funktionalitet og tilsynet med digitale tjenester og fastlægger en grundlæggende struktur for en generel samarbejdsmekanisme mellem medlemsstaterne, som i princippet omfatter alle krav, der gælder for digitale tjenester. Evalueringen af direktivet pegede på mangler ved flere aspekter af denne samarbejdsmekanisme, herunder vigtige proceduremæssige aspekter såsom manglen på klare tidsfrister for medlemsstaternes reaktion kombineret med en generel mangel på reaktionsevne over for anmodninger fra deres modparter. Dette har i årenes løb ført til manglende tillid mellem medlemsstaterne med hensyn til at løse problemer vedrørende udbydere, der tilbyder digitale tjenester på tværs af grænserne. Evalueringen af direktivet viste, at der er behov for at fastsætte et differentieret sæt regler og krav på europæisk plan. Derfor vil gennemførelsen af de specifikke forpligtelser, der er fastsat i denne forordning, kræve en særlig samarbejdsmekanisme på EU-plan med en forvaltningsstruktur, der sikrer koordinering af de specifikke ansvarlige organer på EU-plan.

### 1.5.4. *Forenelighed med den flerårige finansielle ramme og mulige synergivirkninger med andre relevante instrumenter*

Forordningen om harmoniserede regler for kunstig intelligens og om ændring af visse af Unionens lovgivningsmæssige retsakter fastsættes der en ny fælles ramme for krav til AI-systemer, som går langt ud over den ramme, der er fastsat i den

eksisterende lovgivning. Derfor er det med dette forslag nødvendigt at oprette en ny national og europæisk regulerings- og koordineringsfunktion.

Med hensyn til mulige synergier med andre relevante instrumenter kan de bemyndigende myndigheders rolle på nationalt plan varetages af nationale myndigheder, der varetager lignende funktioner i henhold til andre EU-forordninger.

Ved at øge tilliden til kunstig intelligens og dermed tilskynde til investeringer i udvikling og indførelse af kunstig intelligens supplerer den desuden programmet for et digitalt Europa, der som en af fem prioriteter har fremme af udbredelsen af kunstig intelligens.

1.5.5. *Vurdering af de forskellige finansieringsmuligheder, der er til rådighed, herunder muligheden for omfordeling*

Personalet vil blive omfordelt. De øvrige omkostninger vil blive støttet over bevillingsrammen for programmet for et digitalt Europa i betragtning af, at formålet med denne forordning — at sikre pålidelig kunstig intelligens — bidrager direkte til et af hovedmålene for programmet for et digitalt Europa — at fremskynde udviklingen og udbredelsen af kunstig intelligens i Europa.

**1.6. Forslagets/initiativets varighed og finansielle virkninger**

**Begrænset varighed**

- gældende fra [DD/MM]ÅÅÅÅ til [DD/MM]ÅÅÅÅ
- finansielle virkninger fra ÅÅÅÅ til ÅÅÅÅ for forpligtelsesbevillinger og fra ÅÅÅÅ til ÅÅÅÅ for betalingsbevillinger

**Ubegrænset varighed**

- Iværksættelse med en indkøringsperiode på **et/to (bekræftes senere)** år
- derefter gennemførelse i fuldt omfang

**1.7. Planlagt(e) forvaltningsmetode(r)<sup>65</sup>**

**Direkte forvaltning** ved Kommissionen

- i dens tjenestegrene, herunder ved dens personale i EU's delegationer
- i forvaltningsorganerne
- Delt forvaltning** i samarbejde med medlemsstaterne
- Indirekte forvaltning** ved at overlade budgetgennemførelsesopgaver til:
  - tredjelande eller organer, som tredjelande har udpeget
  - internationale organisationer og deres agenturer (angives nærmere)
  - Den Europæiske Investeringsbank og Den Europæiske Investeringsfond
  - de organer, der er omhandlet i finansforordningens artikel 70 og 71
  - offentligretlige organer
  - privatretlige organer, der har fået overdraget samfundsopgaver, forudsat at de stiller tilstrækkelige finansielle garantier

<sup>65</sup> Forklaringer vedrørende forvaltningsmetoder og henvisninger til finansforordningen findes på webstedet BudgWeb: [http://www.cc.ccc/budg/man/budgmanag/budgmanag\\_en.html](http://www.cc.ccc/budg/man/budgmanag/budgmanag_en.html).

- privatretlige organer, undergivet lovgivningen i en medlemsstat, som har fået overdraget gennemførelsen af et offentlig-privat partnerskab, og som stiller tilstrækkelige finansielle garantier
- personer, der har fået overdraget gennemførelsen af specifikke aktioner i den fælles udenrigs- og sikkerhedspolitik i henhold til afsnit V i traktaten om Den Europæiske Union, og som er anført i den relevante basisretsakt
- *Hvis der angives flere forvaltningsmetoder, gives der en nærmere forklaring i afsnittet "Bemærkninger".*

#### Bemærkninger

--

## 2. FORVALTNINGSFORANSTALTNINGER

### 2.1. Bestemmelser om overvågning og rapportering

*Angiv hyppighed og betingelser.*

Forordningen vil blive gennemgået og evalueret fem år efter forordningens ikrafttræden. Kommissionen vil rapportere om evalueringens resultater til Europa-Parlamentet, Rådet og Det Europæiske Økonomiske og Sociale Udvalg.

### 2.2. Forvaltnings- og kontrolsystem(er)

#### 2.2.1. *Begrundelse for den/de foreslåede forvaltningsmetode(r), finansieringsmekanisme(r), betalingsvilkår og kontrolstrategi*

I forordningen fastlægges der en ny politik med hensyn til harmoniserede regler for udbud af systemer med kunstig intelligens på det indre marked, samtidig med at der sikkerheden beskyttes og de grundlæggende rettigheder sikres overholdt. Disse nye regler kræver en sammenhængsmekanisme for anvendelse af forpligtelserne i henhold til denne forordning på tværs af grænserne, som skal tage form af en ny rådgivende gruppe til at koordinere de nationale myndigheders aktiviteter.

For at kunne løse disse nye opgaver er det nødvendigt at afsætte tilstrækkelige ressourcer til Kommissionens tjenestegrene. Håndhævelsen af den nye forordning forventes at kræve 10 fuldtidsækvivalenter (5 fuldtidsækvivalenter til støtte for udvalgets aktiviteter og 5 fuldtidsækvivalenter til Den Europæiske Tilsynsførende for Databeskyttelses funktion som et bemyndigende organ for AI-systemer, der anvendes af EU-organer).

#### 2.2.2. *Oplysninger om de konstaterede risici og det/de interne kontrolsystem(er), der etableres for at afbøde dem*

For at sikre, at udvalgets medlemmer kan foretage velunderbyggede analyser på grundlag af faktuelle oplysninger, fastsættes det, at udvalget bør støttes af Kommissionens administrative struktur, og at der skal nedsættes en ekspertgruppe, der skal yde yderligere ekspertise, når det er nødvendigt.

#### 2.2.3. *Vurdering af og begrundelse for kontrolforanstaltningernes omkostningseffektivitet (forholdet mellem kontrolomkostningerne og værdien af de forvaltede midler) samt vurdering af den forventede risiko for fejl (ved betaling og ved afslutning)*

I betragtning af den lave værdi pr. transaktion (f.eks. godtgørelse af rejseudgifter for en delegeret i forbindelse med et møde) synes standardkontrolprocedurerne for mødeudgifter at være tilstrækkelige. Hvad angår udviklingen af databasen, er tildelingen af kontrakter underlagt et stærkt internt kontrolsystem i GD CNECT gennem centraliserede indkøbsaktiviteter.

### 2.3. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

*Angiv eksisterende eller påtænkte forebyggelses- og beskyttelsesforanstaltninger, f.eks. fra strategien til bekæmpelse af svig.*

De eksisterende foranstaltninger til forebyggelse af svig, der gælder for Kommissionen, vil dække de supplerende bevillinger, der er nødvendige i forbindelse med denne forordning.

### 3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

#### 3.1. Berørt(e) udgiftsområde(r) i den flerårige finansielle ramme og udgiftspost(er) på budgettet

- Eksisterende budgetposter

I samme rækkefølge som udgiftsområderne i den flerårige finansielle ramme og budgetposterne.

Udgiftsområde i den flerårige finansielle ramme	Budgetpost	Udgiftens art OB/IOB <sup>66</sup>	Bidrag			
	Nummer		fra EFTA-lande <sup>67</sup>	fra kandidatlande <sup>68</sup>	fra tredje-lande	iht. finansforordningens artikel 21, stk. 2, litra b)
7	20 02 06 Administrationsudgifter	IOB	NEJ	NEJ	NEJ	NEJ
1	02 04 03 Programmet for et digitalt Europa — Kunstig intelligens	OB	JA	NEJ	NEJ	NEJ
1	02 01 30 01 Udgifter til støttefunktioner i forbindelse med programmet for et digitalt Europa	IOB	JA	NEJ	NEJ	NEJ

#### 3.2. Forslagets anslåede finansielle virkninger for bevillingerne

##### 3.2.1. Sammenfatning af de anslåede virkninger for udgifterne for aktionsbevillingerne

- Forslaget/initiativet medfører ikke anvendelse af aktionsbevillinger
- Forslaget/initiativet medfører anvendelse af aktionsbevillinger som anført herunder:

<sup>66</sup> OB = opdelte bevillinger/IOB = ikke-opdelte bevillinger.

<sup>67</sup> EFTA: Den Europæiske Frihandelssammenslutning.

<sup>68</sup> Kandidatlande og, hvis det er relevant, potentielle kandidatlande på Vestbalkan.

i mio. EUR (tre decimaler)

<b>Udgiftsområde i den flerårige finansielle ramme</b>	1
--	---

GD: CNECT			År 2022	År 2023	År 2024	År 2025	År 2026	År 2027 <sup>69</sup>	I ALT
•Aktionsbevillinger									
Budgetpost <sup>70</sup> 02 04 03	Forpligtelser	(1a)		1,000					1,000
	Betalinger	(2a)		0,600	0,100	0,100	0,100	0,100	1,000
Budgetpost	Forpligtelser	(1b)							
	Betalinger	(2b)							
Administrationsbevillinger finansieret over bevillingsrammen for særprogrammer <sup>71</sup>									
Budgetpost 02 01 30 01		(3)		0,240	0,240	0,240	0,240	0,240	1,200
<b>Bevillinger I ALT til GD CNECT</b>									
	Forpligtelser	=1a+1b+3		1,240		0,240	0,240	0,240	2,200
	Betalinger	=2a+2b+3		0,840	0,340	0,340	0,340	0,340	2,200

<sup>69</sup> Vejledende og afhængig af de disponible budgetmidler.

<sup>70</sup> Ifølge den officielle budgetkontoplan.

<sup>71</sup> Teknisk og/eller administrativ bistand og udgifter til støtte for gennemførelsen af EU's programmer og/eller foranstaltninger (tidligere BA-poster), indirekte forskning, direkte forskning.



• Aktionsbevillinger I ALT	Forpligtelser	(4)		1,000							<b>1,000</b>
	Betalinger	(5)		0,600	0,100	0,100	0,100	0,100			<b>1,000</b>
• Administrationsbevillinger finansieret over bevillingsrammen for særprogrammer I ALT		(6)		<b>0,240</b>	<b>0,240</b>	<b>0,240</b>	<b>0,240</b>	<b>0,240</b>			<b>1,200</b>
<b>Bevillinger I ALT under UDGIFTSOMRÅDE 1</b> i den flerårige finansielle ramme		Forpligtelser	=4+6	1,240	0,240	0,240	0,240	0,240			<b>2,200</b>
		Betalinger	=5+6	0,840	0,340	0,340	0,340	0,340			<b>2,200</b>

**Hvis flere udgiftsområder berøres af forslaget/initiativet, indsættes der et tilsvarende afsnit for hvert udgiftsområde**

• Aktionsbevillinger I ALT (alle aktionsrelaterede udgiftsområder)	Forpligtelser	(4)									
	Betalinger	(5)									
• Administrationsbevillinger finansieret over bevillingsrammen for særprogrammer I ALT (alle aktionsrelaterede udgiftsområder)		(6)									
<b>Bevillinger I ALT under UDGIFTSOMRÅDE 1-6</b> i den flerårige finansielle ramme (referencebeløb)		Forpligtelser	=4+6								
		Betalinger	=5+6								

<b>Udgiftsområde i den flerårige finansielle ramme</b>	<b>7</b>	"Administrationsudgifter"
--	----------	---------------------------

Dette afsnit skal udfyldes ved hjælp af arket vedrørende administrative budgetoplysninger, der først skal indføres i [bilaget til finansieringsoversigten](#) (bilag V til de interne regler), som uploades til DECIDE med henblik på høring af andre tjenestegrene.

i mio. EUR (tre decimaler)

		År 2023	År 2024	År 2025	År 2026	År 2027	Efter 2027 <sup>72</sup>	I ALT
GD: CNECT								
• Menneskelige ressourcer		0,760	0,760	0,760	0,760	0,760	0,760	<b>3,800</b>
• Andre administrationsudgifter		<b>0,010</b>	<b>0,010</b>	<b>0,010</b>	<b>0,010</b>	<b>0,010</b>	<b>0,010</b>	<b>0,050</b>
<b>I ALT GD CNECT</b>		<b>0,760</b>	<b>0,760</b>	<b>0,760</b>	<b>0,760</b>	<b>0,760</b>	<b>0,760</b>	<b>3,850</b>
Den Europæiske Tilsynsførende for Databeskyttelse (EDPS)								
• Menneskelige ressourcer		0,760	0,760	0,760	0,760	0,760	0,760	<b>3,800</b>
• Andre administrationsudgifter								
<b>I ALT EDPS</b>		<b>0,760</b>	<b>0,760</b>	<b>0,760</b>	<b>0,760</b>	<b>0,760</b>	<b>0,760</b>	<b>3,800</b>
<b>Bevillinger I ALT under UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme</b>		(Forpligtelser i alt = betalinger i alt)		1,530	1,530	1,530	1,530	<b>7,650</b>

i mio. EUR (tre decimaler)

		År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	I ALT
<b>Bevillinger I ALT under UDGIFTSOMRÅDE 1-7 i den flerårige finansielle ramme</b>		Forpligtelser	2,770	1,770	1,770	1,770	1,770	<b>9,850</b>
		Betalinger	2,370	1,870	1,870	1,870	1,870	<b>9,850</b>

<sup>72</sup>

Alle tal i denne kolonne er vejledende og afhænger af videreførelsen af programmerne og disponible bevillinger.

3.2.2. Anslåede resultater finansieret med aktionsbevillinger

Forpligtelsesbevillinger i mio. EUR (tre decimaler)

Angiv mål og resultater ↓			År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	Efter 2027 <sup>73</sup>	I ALT									
<b>RESULTATER</b>																			
Type	Gnsntl. omkost- ninger	Antal	Om- kost- ninger	Antal	Om- kost- ninger	Antal	Om- kost- ninger	Antal	Om- kost- ninger	Antal	Om- kost- ninger	Antal	Om- kost- ninger	Antal	Om- kost- ninger	Antal	Om- kost- ninger	Anta l resul- tater i alt	Om- kost- ninger i alt
SPECIFIKT MÅL NR. 1 <sup>74</sup> ...																			
Database				1	1,000	1		1		1		1		1	0,100	1	1,000		
Møder — Resultat				10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Kommunikationsakti- viteter				2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Subtotal for specifikt mål nr. 1																			
SPECIFIKT MÅL NR. 2																			
- Resultat																			
Subtotal for specifikt mål nr. 2																			
<b>I ALT</b>				13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200		

<sup>73</sup> Alle tal i denne kolonne er vejledende og afhænger af videreførelsen af programmerne og disponible bevillinger.

<sup>74</sup> Som beskrevet i punkt 1.4.2. "Specifikt/specifikke mål".

### 3.2.3. Sammenfatning af de anslåede virkninger for administrationsbevillingerne

- Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger
- Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	Årligt efter 2027 <sup>75</sup>	I ALT
--	------------	------------	------------	------------	------------	------------	------------------------------------	-------

<b>UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme</b>								
Menneskelige ressourcer		1,520	1,520	1,520	1,520	1,520	<b>1,520</b>	<b>7,600</b>
Andre administrationsudgifter		0,010	0,010	0,010	0,010	0,010	<b>0,010</b>	<b>0,050</b>
<b>Subtotal UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme</b>		1,530	1,530	1,530	1,530	1,530	<b>1,530</b>	<b>7,650</b>

<b>Uden for UDGIFTSOMRÅDE 7<sup>76</sup> of the i den flerårige finansielle ramme</b>								
Menneskelige ressourcer								
Andre administrationsudgifter		0,240	0,240	0,240	0,240	0,240	<b>0,240</b>	<b>1,20</b>
<b>Subtotal uden for UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme</b>		0,240	0,240	0,240	0,240	0,240	<b>0,240</b>	<b>1,20</b>

<b>I ALT</b>		<b>1,770</b>	<b>1,770</b>	<b>1,770</b>	<b>1,770</b>	<b>1,770</b>	<b>1,770</b>	<b>8,850</b>
--------------	--	--------------	--------------	--------------	--------------	--------------	--------------	--------------

Bevillingerne til menneskelige ressourcer og andre administrationsudgifter vil blive dækket ved hjælp af de bevillinger, som generaldirektoratet allerede har afsat til forvaltning af foranstaltningen, og/eller ved intern omfordeling i generaldirektoratet, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige generaldirektorat i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

<sup>75</sup> Alle tal i denne kolonne er vejledende og afhænger af videreførelsen af programmerne og disponible bevillinger.

<sup>76</sup> Teknisk og/eller administrativ bistand og udgifter til støtte for gennemførelsen af EU's programmer og/eller foranstaltninger (tidligere BA-poster), indirekte forskning, direkte forskning.

### 3.2.3.1. Anslået behov for menneskelige ressourcer

- Forslaget/initiativet medfører ikke anvendelse af menneskelige ressourcer
- Forslaget/initiativet medfører anvendelse af menneskelige ressourcer som anført herunder:

*Overslag angives i årsværk*

	År 2023	År 2024	År 2025	2026	2027	Efter 2027 <sup>77</sup>	
<b>• Stillinger i stillingsfortegnelsen (tjenestemænd og midlertidigt ansatte)</b>							
20 01 02 01 (i Kommissionens hovedsæde og repræsentationskontorer)	10	10	10	10	10	10	
20 01 02 03 (i delegationerne)							
01 01 01 01 (indirekte forskning)							
01 01 01 11 (direkte forskning)							
Andre budgetposter (angiv nærmere)							
<b>• Eksternt personale (i årsværk)<sup>78</sup></b>							
20 02 01 (KA, UNE, V under den samlede bevillingsramme)							
20 02 03 (KA, LA, UNE, V og JMD i delegationerne)							
<b>XX 01 xx yy zz</b> <sup>79</sup>	- i hovedsædet						
	- i delegationerne						
01 01 01 02 (KA, UNE, V – indirekte forskning)							
01 01 01 12 (KA, UNE, V – direkte forskning)							
Andre budgetposter (skal angives)							
<b>I ALT</b>	<b>10</b>	<b>10</b>	<b>10</b>	<b>10</b>	<b>10</b>	<b>10</b>	

**XX** angiver det berørte politikområde eller budgetafsnit.

Personalebehovet vil blive dækket ved hjælp af det personale, som generaldirektoratet allerede har afsat til forvaltning af foranstaltningen, og/eller ved interne rokader i generaldirektoratet, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige generaldirektorat i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

EDPS forventes at stille halvdelen af de nødvendige ressourcer til rådighed.

#### Opgavebeskrivelse:

Tjenestemænd og midlertidigt ansatte	<p>Forberedelsen af i alt 13-16 møder, udkast til rapporter, det politiske arbejde (f.eks. vedrørende fremtidige ændringer af listen over højrisiko-AI-anvendelser) og varetagelse af forbindelserne med medlemsstaternes myndigheder vil kræve fire AD-fuldtidsækvivalenter og én AST-fuldtidsækvivalent.</p> <p>Den Europæiske Tilsynsførende for Databeskyttelse er ansvarlig for AI-systemer udviklet af EU-institutionerne. På grundlag af tidligere erfaringer kan det anslås, at der kræves fem AD-fuldtidsækvivalenter for at opfylde Den Europæiske Tilsynsførende</p>
--------------------------------------	---

<sup>77</sup> Alle tal i denne kolonne er vejledende og afhænger af videreførelsen af programmerne og disponible bevillinger.

<sup>78</sup> KA: kontraktansatte, LA: lokalt ansatte, UNE: udstationerede nationale eksperter, V: vikarer, JMD: juniormedarbejdere i delegationerne.

<sup>79</sup> Delloft for eksternt personale under aktionsbevillingerne (tidligere BA-poster).

	for Databeskyttelse ansvar i henhold til lovgivningsudkastet.
Eksternt personale	

### 3.2.4. Forenelighed med indeværende flerårige finansielle ramme

Forslaget/initiativet:

- kan finansieres fuldt ud gennem omfordeling inden for det relevante udgiftsområde i den flerårige finansielle ramme (FFR)

Der er ikke behov for omlægning.

- kræver anvendelse af den uudnyttede margen under det relevante udgiftsområde i FFR og/eller anvendelse af særlige instrumenter som fastlagt i FFR-forordningen

Gør rede for behovet med angivelse af de berørte udgiftsområder og budgetposter, de beløb, der er tale om, og de instrumenter, der foreslås anvendt.

- kræver en revision af FFR

Gør rede for behovet med angivelse af de berørte udgiftsområder og budgetposter og de beløb, der er tale om.

### 3.2.5. Bidrag fra tredjemand

Forslaget/initiativet:

- indeholder ikke bestemmelser om samfinansiering med tredjemand
- indeholder bestemmelser om samfinansiering med tredjemand, jf. følgende overslag:

Bevillinger i mio. EUR (tre decimaler)

	År n <sup>80</sup>	År n+1	År n+2	År n+3	Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)			I alt
Angiv det organ, der deltager i samfinansieringen								
Samfinansierede bevillinger I ALT								

<sup>80</sup> År n er det år, hvor gennemførelsen af forslaget/initiativet påbegyndes. Erstat "n" med det forventede første gennemførelsesår (f.eks.: 2021). Dette gælder også for de efterfølgende år.

### 3.3. Anslåede virkninger for indtægterne

- Forslaget/initiativet har følgende finansielle virkninger:
- Forslaget/initiativet har følgende finansielle virkninger:
  - for andre indtægter
  - for andre indtægter
  - Angiv, om indtægterne er formålsbestemte

i mio. EUR (tre decimaler)

Indtægtspost på budgettet	Bevillinger til rådighed i indeværende regnskabsår	Forslagets/initiativets virkninger <sup>81</sup>					Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)	
		År n	År n+1	År n+2	År n+3			
Artikel ...								

For indtægter, der er formålsbestemte, angives det, hvilke af budgettets udgiftsposter der berøres.

Andre bemærkninger (f.eks. om hvilken metode, der er benyttet til at beregne virkningerne for indtægterne).

<sup>81</sup> Med hensyn til EU's traditionelle egne indtægter (told og sukkerafgifter) opgives beløbene netto, dvs. bruttobeløb, hvorfra der er trukket opkrævningsomkostninger på 20 %.