

Bruxelles, den 6. december 2022
(OR. en)

15698/22

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

**TELECOM 516
JAI 1633
COPEN 434
CYBER 399
DATAPROTECT 351
EJUSTICE 95
COSI 318
IXIM 291
ENFOPOL 626
RELEX 1674
MI 918
COMPET 1005
CODEC 1940**

RESULTAT AF DRØFTELSENE

fra:	Generalsekretariatet for Rådet
dato:	6. december 2022
til:	delegationerne
Tidl. dok. nr.:	14954/22 + ADD 1
Komm. dok. nr.:	8115/21
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 – Generel indstilling (den 6. december 2022)

Vedlagt følger til delegationerne Rådets generelle indstilling til ovennævnte forslag som godkendt af Rådet (transport, telekommunikation og energi) på 3917. samling den 6. december 2022.

Den generelle indstilling fastlægger Rådets foreløbige holdning til dette forslag og danner grundlag for forberedelserne af forhandlingerne med Europa-Parlamentet.

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**

(EØS-relevant tekst)

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 Udvalg¹,

under henvisning til udtalelse fra Regionsudvalget²,

under henvisning til udtalelse fra Den Europæiske Centralbank³,

efter den almindelige lovgivningsprocedure, og

ud fra følgende betragtninger:

¹ EUT C [...] af [...], s. [...].

² EUT C [...] af [...], s. [...].

³ Henvisning til ECB-udtalelse.

- (1) Formålet med denne forordning er at forbedre det indre markedes 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, importerer 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 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. Sådan 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 fastsættelsen af disse regler og viderebygningen på arbejdet i Ekspertgruppen på Højt Niveau vedrørende Kunstig Intelligens som afspejlet i retningslinjerne for pålidelig kunstig intelligens i EU 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 Råd⁴, og der sikres beskyttelse af etiske principper, som Europa-Parlamentet specifikt har anmodet om⁵.

⁴ Det Europæiske Råd, Ekstraordinært møde i Det Europæiske Råd (1. og 2. oktober 2020) – Konklusioner, EUCO 13/20, 2020, s. 6.

⁵ 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).

- (5a) De harmoniserede regler om omsætning, ibrugtagning og anvendelse af AI-systemer, der er fastsat i denne forordning, bør finde anvendelse på tværs af sektorer og bør i overensstemmelse med tilgangen med den nye lovgivningsmæssige ramme ikke berøre eksisterende EU-ret, navnlig om databeskyttelse, forbrugerbeskyttelse, grundlæggende rettigheder, beskæftigelse og produktsikkerhed, som denne forordning supplerer. Som følge heraf forbliver alle rettigheder og retsmidler, som en sådan EU-ret giver forbrugere og andre personer, som kan blive negativt påvirket af AI-systemer, herunder for så vidt angår erstatning for eventuelle skader i henhold til Rådets direktiv 85/374/EØF af 25. juli 1985 om tilnærmelse af medlemsstaternes administrativt eller ved lov fastsatte bestemmelser om produktansvar, uberørte og finder fuldt ud anvendelse. Derudover har denne forordning til formål at styrke effektiviteten af sådanne eksisterende rettigheder og retsmidler ved at fastsætte specifikke krav og forpligtelser, herunder med hensyn til gennemsigtighed, teknisk dokumentation og registrering af AI-systemer. Desuden bør de forpligtelser, der pålægges forskellige operatører, der er involveret i AI-værdikæden i henhold til denne forordning, finde anvendelse med forbehold af national lovgivning i overensstemmelse med EU-retten, hvormed anvendelsen af visse AI-systemer begrænses, hvis en sådan lovgivning falder uden for denne forordnings anvendelsesområde eller forfølger andre legitime mål af samfundsmæssig interesse end dem, der forfølges med denne forordning. F.eks. bør national arbejdsret og lovgivningen om beskyttelse af mindreårige (dvs. personer under 18 år) under hensyntagen til FN's generelle bemærkning nr. 25 (2021) om børns rettigheder, for så vidt som de ikke er specifikke for AI-systemer og forfølger andre mål af almen interesse, ikke berøres af denne forordning.

- (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 centrale funktionelle karakteristika ved kunstig intelligens såsom dens lærings-, ræsonnements- eller modelleringskapacitet, idet den adskiller den fra enklere softwaresystemer og programmeringstilgange. Navnlig i forbindelse med denne forordning bør AI-systemer have evnen til, på grundlag af maskin- og/eller menneskebaserede data og input, at udlede en måde, hvorpå der kan opnås et sæt endelige mål, som mennesker har givet dem, ved hjælp af maskinlæring og/eller logiske og videnbaserede tilgange, og til at producere output såsom indhold til generative AI-systemer (f.eks. tekst, video eller billeder), forudsigelser, anbefalinger eller beslutninger, der påvirker det miljø, som systemet interagerer med, hvad enten det er i en fysisk eller digital dimension. Et system, der anvender regler, der udelukkende er defineret af fysiske personer til automatisk at udføre operationer, bør ikke betragtes som et AI-system. 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). Begrebet "et AI-systems autonomi" vedrører, i hvilken grad et sådant system fungerer uden menneskelig medvirken.
- (6a) Maskinlæringstilgange fokuserer på udvikling af systemer, der er i stand til at lære og drage slutninger af data for at løse et applikationsproblem uden udtrykkeligt at være programmeret med et sæt trinvis instrukser fra input til output. Læring henviser til den beregningsproces, der består i at optimere modellens parametre ud fra data, hvilket er en matematisk konstruktion, der genererer et output baseret på inputdata. Den vifte af problemer, der behandles ved maskinlæring, omfatter typisk opgaver, som andre tilgange ikke kan løse, enten fordi problemet ikke er formaliseret på passende vis, eller fordi problemet er vanskeligt at behandle med ikkelæringsmæssige tilgange. Maskinlæringstilgange omfatter f.eks. superviseret, usuperviseret og reinforcement learning ved hjælp af en række metoder, herunder dyb læring med neurale netværk, statistiske teknikker til læring og inferens (herunder f.eks. logistisk regression og bayesiansk estimation), og søgnings- og optimeringsmetoder.

- (6b) Logiske og videnbaserede tilgange fokuserer på udvikling af systemer med logisk ræsonnementskapacitet vedrørende viden med henblik på at løse et applikationsproblem. Sådanne systemer omfatter typisk en videnbase og en inferensmotor, der genererer output ved hjælp af ræsonnement på grundlag af videnbasen. Videnbasen, som normalt indkodes af eksperter, repræsenterer enheder og logiske forhold, der er relevante for applikationsproblemet, gennem formalisme baseret på regler, ontologier eller videngrafer. Inferensmotoren virker på videnbasen og udtrækker nye oplysninger gennem operationer såsom sortering, søgning, matchning eller kædning. Logiske og videnbaserede tilgange omfatter f.eks. videnrepræsentation, induktiv (logisk) programmering, videnbaser, inferens- og deduktionsmotorer, (symbolsk) ræsonnement, ekspertsystemer og søgnings- og optimeringsmetoder.
- (6c) For at sikre ensartede betingelser for gennemførelsen af denne forordning for så vidt angår maskinlæringstilgange og logiske og videnbaserede tilgange og for at tage hensyn til den markedsmæssige og teknologiske udvikling bør Kommissionen tillægges gennemførelsesbeføjelser.
- (6d) Begrebet "bruger" som omhandlet i denne forordning bør fortolkes som enhver fysisk eller juridisk person, herunder en offentlig myndighed, et agentur eller et andet organ, der anvender et AI-system, under hvis myndighed systemet anvendes. Afhængigt af typen af AI-system kan anvendelsen af systemet påvirke andre personer end brugeren.

- (7) Begrebet biometriske data, der anvendes i denne forordning, bør fortolkes i overensstemmelse med begrebet biometriske data som defineret i artikel 4, stk. 14, i Europa-Parlamentets og Rådets forordning (EU) 2016/679⁶, artikel 3, stk. 18, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725⁷ og artikel 3, stk. 13, i Europa-Parlamentets og Rådets direktiv (EU) 2016/680⁸.

⁶ 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).

⁷ 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).

⁸ 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).

- (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 typisk på afstand uden deres aktive medvirken ved at sammenligne en persons biometriske data med de biometriske data i et referencedataregister, uanset hvilken teknologi, hvilke processer eller hvilke typer biometriske data der anvendes. Sådanne systemer til biometrisk fjernidentifikation anvendes typisk til at opfatte (scanne) flere personer eller deres adfærd samtidigt for i væsentlig grad at lette identifikationen af en række personer uden deres aktive medvirken. En sådan definition udelukker kontrol- og autentifikationssystemer, hvis eneste formål er at bekræfte, at en bestemt fysisk person er den person, vedkommende hævder at være, samt systemer, der anvendes til at bekræfte en fysisk persons identitet udelukkende med det formål at få adgang til en tjeneste, en anordning eller lokaler. Denne udelukkelse begrundes med, at sådanne systemer sandsynligvis vil have en mindre indvirkning på fysiske personers grundlæggende rettigheder sammenlignet med systemer til biometrisk fjernidentifikation, der kan anvendes til behandling af et stort antal personers biometriske data. 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 et ubestemt antal fysiske personer, og uanset om det pågældende sted er privatejet eller offentligt ejet, og uanset den aktivitet, som stedet kan anvendes til, såsom handel (f.eks. butikker, restauranter, caféer), tjenesteydelser (f.eks. banker, erhvervsmæssige aktiviteter, hotel-, restaurations- og oplevelsesbranchen), sport (f.eks. svømmebassiner, fitnesscentre, stadioner), transport (f.eks. bus-, metro- og jernbanestationer, lufthavne, transportmidler), underholdning (f.eks. biografer, teatre, museer, koncert- og konferencesale) fritid eller andet (f.eks. offentlige veje og pladser, parker, skove, legepladser). Et sted bør også klassificeres som offentligt sted, hvis adgangen, uanset eventuelle kapacitets- eller sikkerhedsrestriktioner, er underlagt visse forud fastsatte betingelser, som kan opfyldes af et ubestemt antal personer, såsom køb af en billet eller et rejsebevis, forudgående registrering eller en bestemt alder. Derimod bør et sted ikke anses for at være et offentligt sted, hvis adgangen er begrænset til specifikke og definerede fysiske personer i henhold til enten EU-retten eller national ret, der er direkte knyttet til den offentlige sikkerhed, eller gennem en klar viljestilkendegivelse fra den person, der har den relevante beføjelse på stedet. Den faktiske mulighed for adgang alene (f.eks. en ulåst dør, en åben port i et hegn) indebærer ikke, at stedet er et offentligt sted, hvis der er indikationer eller omstændigheder, der antyder det modsatte (f.eks. skilte, der forbyder eller begrænser adgangen). Virksomheds- og fabrikslokaler samt kontorer og arbejdspladser, der kun skal tilgås af relevante medarbejdere og tjenesteydere, er ikke offentlige steder. Offentlige steder bør ikke omfatte fængsler eller grænsekontrolområder. Andre områder kan bestå af både ikkeoffentlige steder og offentlige steder, som f.eks. forhallen til en privat beboelsesejendom, der er nødvendig at gå igennem for at få adgang til en læges kontor, eller en lufthavn. Online steder er heller ikke omfattet, da der ikke er tale om fysiske steder. 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. 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 fremtidigt 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. De modtagende medlemsstaters myndigheder og Unionens institutioner, kontorer, organer og organer, der gør brug af sådanne output i Unionen, forbliver ansvarlige for at sikre, at deres anvendelse er i overensstemmelse med EU-retten. Når disse internationale aftaler revideres, eller der indgås nye i fremtiden, bør de kontraherende parter gøre deres yderste for at tilpasse disse aftaler til kravene i denne forordning.
- (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.

(-12a) Hvis og i det omfang AI-systemer bringes i omsætning, tages i brug eller anvendes med eller uden ændringer af sådanne systemer til militær-, forsvars- eller nationale sikkerhedsformål, bør disse udelukkes fra denne forordnings anvendelsesområde, uanset hvilken type enhed der udfører disse aktiviteter, f.eks. om det er en offentlig eller privat enhed. For så vidt angår militære og forsvarsmæssige formål begrundes en sådan udelukkelse både i medfør af artikel 4, stk. 2, i TEU, og i de særlige forhold, der gør sig gældende for medlemsstaternes forsvarspolitik og den fælles EU-forsvarspolitik, der er omfattet af afsnit V, kapitel 2, i traktaten om Den Europæiske Union (TEU), og som er underlagt folkeretten, og som derfor er den mest hensigtsmæssige retlige ramme for regulering af AI-systemer i forbindelse med anvendelsen af dødbringende magtanvendelse og andre AI-systemer i forbindelse med militære og forsvarsmæssige aktiviteter. For så vidt angår nationale sikkerhedsformål begrundes udelukkelsen både i den omstændighed, at den nationale sikkerhed forbliver medlemsstaternes eneansvar i overensstemmelse med artikel 4, stk. 2, i TEU, og i den særlige karakter af og de operationelle behov i forbindelse med nationale sikkerhedsaktiviteter og specifikke nationale regler, der finder anvendelse på disse aktiviteter. Hvis et AI-system, der er udviklet, bragt i omsætning, taget i brug eller anvendt til militær-, forsvars- eller nationale sikkerhedsformål, anvendes uden for disse midlertidigt eller permanent til andre formål (f.eks. civile eller humanitære formål, retshåndhævelsesformål eller hensynet til den offentlige sikkerhed), vil et sådant system ikke desto mindre være omfattet af denne forordnings anvendelsesområde. I så fald bør den enhed, der anvender systemet til andre formål end militær-, forsvars- eller nationale sikkerhedsformål, sikre, at systemet er i overensstemmelse med denne forordning, medmindre systemet allerede er i overensstemmelse med denne forordning. AI-systemer, der bringes i omsætning eller tages i brug til et udelukket formål (dvs. militær-, forsvars- eller nationale sikkerhedsformål) og et eller flere ikkeudelukkede formål (f.eks. civile formål, retshåndhævelse osv.), falder ind under denne forordnings anvendelsesområde, og udbydere af disse systemer bør sikre overholdelse af denne forordning. I disse tilfælde bør det forhold, at et AI-system kan være omfattet af denne forordnings anvendelsesområde, ikke berøre muligheden for, at enheder, der udfører nationale sikkerheds-, forsvars- og militæraktiviteter, uanset hvilken type enhed der udfører disse aktiviteter, anvender AI-systemer til nationale sikkerheds-, militær- og forsvarsformål, hvis anvendelse er udelukket fra denne forordnings anvendelsesområde. Et AI-system, der bringes i omsætning til civile formål eller retshåndhævelsesformål, og som anvendes med eller uden ændringer til militær-, forsvars- eller nationale sikkerhedsformål, bør ikke være omfattet af denne forordnings anvendelsesområde, uanset hvilken type enhed der udfører disse aktiviteter.

- (12a) 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].
- (12b) Denne forordning bør ikke undergrave forsknings- og udviklingsaktiviteter og bør respektere forskningsfriheden. Det er derfor nødvendigt at udelukke AI-systemer, der er specifikt udviklet og taget i brug udelukkende med henblik på videnskabelig forskning og udvikling, fra forordningens anvendelsesområde og sikre, at den ikke på anden måde påvirker videnskabelig forskning og udvikling af AI-systemer. Med hensyn til udbydernes produktorienterede forskningsaktiviteter bør bestemmelserne i denne forordning heller ikke finde anvendelse. Dette berører ikke forpligtelsen til at overholde denne forordning, når et AI-system, der falder ind under denne forordnings anvendelsesområde, bringes i omsætning eller tages i brug som følge af en sådan forsknings- og udviklingsaktivitet, eller anvendelsen af bestemmelser om reguleringsmæssige sandkasser og prøvning under faktiske forhold. Uden at det berører ovenstående vedrørende AI-systemer, der specifikt er udviklet og taget i brug udelukkende med henblik på videnskabelig forskning og udvikling, bør ethvert andet AI-system, der kan anvendes til udførelse af enhver forsknings- og udviklingsaktivitet, desuden fortsat være omfattet af bestemmelserne i denne forordning. Under alle omstændigheder bør alle forsknings- og udviklingsaktiviteter udføres i overensstemmelse med anerkendte etiske og professionelle standarder for videnskabelig forskning.

(12c) I lyset af arten og kompleksiteten af værdikæden for AI-systemer er det vigtigt at præcisere den rolle, som aktører, der kan bidrage til udviklingen af AI-systemer, navnlig højrisiko-AI-systemer, spiller. Det er navnlig nødvendigt at præcisere, at AI-systemer til generelle formål er AI-systemer, der af udbyderen er beregnet til at udføre almindeligt anvendelige funktioner såsom billed- og talegenkendelse og i en lang række sammenhænge. De kan anvendes som højrisiko-AI-systemer i sig selv eller som komponenter i andre højrisiko-AI-systemer. Derfor bør sådanne systemer på grund af deres særlige karakter og for at sikre en rimelig ansvarsfordeling i hele AI-værdikæden være underlagt forholdsmæssige og mere specifikke krav og forpligtelser i henhold til denne forordning, samtidig med at der sikres et højt beskyttelsesniveau for grundlæggende rettigheder, sundhed og sikkerhed. Desuden bør udbydere af AI-systemer til generelle formål, uanset om de kan anvendes som højrisiko-AI-systemer som sådan af andre udbydere eller som komponenter i højrisiko-AI-systemer, alt efter hvad der er relevant, samarbejde med udbyderne af de respektive højrisiko-AI-systemer for at gøre det muligt for dem at overholde de relevante forpligtelser i henhold til denne forordning og med de kompetente myndigheder, der er oprettet i henhold til denne forordning. For at tage hensyn til de særlige karakteristika ved AI-systemer til generelle formål og den hastigt skiftende markedsmæssige og teknologiske udvikling på området bør Kommissionen tillægges gennemførelsesbeføjelser til at præcisere og tilpasse anvendelsen af de krav, der er fastsat i denne forordning, til AI-systemer til generelle formål og til at præcisere, hvilke oplysninger udbydere af AI-systemer til generelle formål skal dele, for at gøre det muligt for udbyderne af det respektive højrisiko-AI-system at opfylde deres forpligtelser i henhold til denne forordning.

- (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 ikkediskriminerende 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 gennemsigtighedsforpligtelser 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. Sådant 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) AI-baserede manipulerende teknikker kan anvendes til at overtale personer til at udvise uønsket adfærd eller til at vildlede dem ved at nudge dem til at træffe beslutninger på en måde, der undergraver og hæmmer deres autonomi, beslutningstagning og frie valg. Omsætning, ibrugtagning eller anvendelse af visse AI-systemer, der i væsentlig grad fordrejer menneskers adfærd, og hvor der er sandsynlighed for fysiske eller psykiske skader, er særligt farlige og bør derfor forbydes. Sådanne AI-systemer anvender subliminale komponenter såsom lyd-, billede- eller videostimuli, som mennesker ikke kan opfatte, eftersom disse stimuli ligger uden for den menneskelige opfattelse, eller andre subliminale teknikker, der undergraver eller hæmmer menneskers autonomi, beslutningstagning eller frie valg på måder, som folk ikke bevidst er klar over, eller, selv om de er klar over det, ikke er i stand til at kontrollere eller modstå, f.eks. i tilfælde af grænseflader mellem maskine og hjerne eller virtuel virkelighed. Desuden kan AI-systemer også på anden måde udnytte sårbarheder hos en specifik gruppe af mennesker på grund af deres alder, handicap som omhandlet i direktiv (EU) 2019/882 eller en specifik social eller økonomisk situation, der sandsynligvis vil gøre disse personer mere sårbare over for udnyttelse, såsom personer, der lever i ekstrem fattigdom eller i etniske eller religiøse mindretal. Sådanne AI-systemer kan bringes i omsætning, tages i brug eller anvendes med den hensigt eller det resultat i væsentlig grad at fordreje en persons adfærd og på en måde, der forvolder eller med rimelighed kan forventes at ville forvolde den pågældende eller en anden person eller persongrupper fysisk eller psykisk skade, herunder skade, der kan akkumuleres over tid. Hensigten om at fordreje adfærden kan ikke formodes, hvis fordrejningen af menneskelig adfærd skyldes faktorer, som ligger uden for AI-systemet og uden for udbyderens eller brugerens kontrol, dvs. faktorer, der ikke med rimelighed kan forventes og afbødes af udbyderen eller brugeren af AI-systemet. Under alle omstændigheder er det ikke nødvendigt for udbyderen eller brugeren at have til hensigt at forårsage fysisk eller psykisk skade, når en sådan skade er resultatet af AI-baseret manipulativ eller udnyttende praksis. Forbuddene mod en sådan AI-praksis supplerer bestemmelserne i direktiv 2005/29/EF, navnlig at urimelig handelspraksis, der påfører forbrugerne økonomisk eller finansiell skade, er forbudt under alle omstændigheder, uanset om den indføres ved hjælp af AI-systemer eller på anden måde. Forbuddene mod manipulativ og udnyttende praksis i denne forordning bør ikke berøre lovlig praksis i forbindelse med lægebehandling såsom psykologbehandling af psykisk sygdom eller fysisk rehabilitering, når disse praksisser udføres i overensstemmelse med gældende medicinske standarder og lovgivning. Desuden bør almindelig og legitim handelspraksis, der er i overensstemmelse med gældende ret, ikke i sig selv anses for at udgøre skadelig manipulerende AI-praksis.

- (17) AI-systemer, der af offentlige myndigheder eller af private aktører gør 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 personer 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. AI-systemer, der medfører en sådan uacceptabel pointpraksis, bør derfor forbydes. Dette forbud bør ikke berøre en lovlig praksis med evaluering af fysiske personer, der udføres med et eller flere specifikke formål i overensstemmelse med loven.
- (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 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/JHA⁹, 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 lovovertrædelsen 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 lovovertrædelsens alvor, omfang eller mulige negative konsekvenser. Desuden bør denne forordning bevare de retshåndhævende myndigheders, grænsekontrolmyndighedernes, indvandringsmyndighedernes eller asylmyndighedernes mulighed for at foretage identitetskontrol under tilstedeværelse af den pågældende person i overensstemmelse med de betingelser, der er fastsat i EU-retten og national ret for en sådan kontrol. Navnlig bør retshåndhævende myndigheder, grænsekontrolmyndigheder, indvandringsmyndigheder eller asylmyndigheder kunne anvende informationssystemer i overensstemmelse med EU-retten eller national ret til at identificere en person, der under en identitetskontrol enten nægter at blive identificeret eller ikke er i stand til at oplyse eller bevise sin identitet, uden at det i henhold til denne forordning kræves, at der indhentes forhåndstilladelse. Dette kan f.eks. være en person, der er involveret i en forbrydelse, og som er uvillig eller ude af stand til på grund af en ulykke eller en helbredstilstand at afsløre sin identitet over for de retshåndhævende myndigheder.

⁹ 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).

- (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 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 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 af systemet med henblik på at identificere en eller flere personer. Undtagelser fra denne regel bør tillades 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.

- (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 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, bør fortsat opfylde alle krav, der følger af artikel 10 i direktiv (EU) 2016/680. Med henblik på andre formål end retshåndhævelse forbyder artikel 9, stk. 1, i forordning (EU) 2016/679 og artikel 10, stk. 1, i forordning (EU) 2018/1725 behandling af biometriske data med det formål entydigt at identificere en fysisk person, medmindre en af situationerne i de respektive stk. 2 i disse to artikler finder anvendelse.
- (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, 3 og 4 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, 3 og 4 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. 300/2008¹⁰, Europa-Parlamentets og Rådets forordning (EU) nr. 167/2013¹¹, Europa-Parlamentets og Rådets forordning (EU) nr. 168/2013¹², Europa-Parlamentets og Rådets direktiv 2014/90/EU¹³, Europa-Parlamentets og Rådets direktiv (EU) 2016/797¹⁴, Europa-Parlamentets og Rådets forordning (EU) 2018/858¹⁵, Europa-Parlamentets og Rådets forordning (EU) 2018/1139¹⁶ og Europa-Parlamentets og Rådets forordning (EU) 2019/2144¹⁷, 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.

¹⁰ 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).

¹¹ 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).

¹² 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).

¹³ 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).

¹⁴ 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).

¹⁵ 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).

¹⁶ 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).

¹⁷ 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 forordning (EF) nr. 78/2009, forordning (EF) nr. 79/2009 og Europa-Parlamentets og Rådets forordning (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).

- (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 sikringssystemer 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 tilfældet med Europa-Parlamentets og Rådets forordning (EU) 2017/745¹⁸ og Europa-Parlamentets og Rådets forordning (EU) 2017/746¹⁹, hvor en tredjepart foretager overensstemmelsesvurderinger af mellemrisiko- og højrisikoprodukter.

¹⁸ 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).

¹⁹ 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).

- (32) 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. Det er også vigtigt at præcisere, at der inden for de højrisikoscenarier, der er omhandlet i bilag III, kan være systemer, der ikke medfører en væsentlig risiko for de retlige interesser, der beskyttes i disse scenarier, under hensyntagen til det output, der produceres af AI-systemet. Derfor bør det AI-system, der genererer et sådant output, kun anses for at udgøre en høj risiko, når outputtet har stor betydning (dvs. ikke er rent accessorisk) i forhold til den relevante foranstaltning eller beslutning med hensyn til at skabe en betydelig risiko for de beskyttede retlige interesser. Når de oplysninger, som et menneske får fra et AI-system eksempelvis består i profilering af fysiske personer som omhandlet i artikel 4, stk. 4, i forordning (EU) 2016/679, artikel 3, stk. 4, i direktiv (EU) 2016/680 og artikel 3, stk. 5, i forordning (EU) 2018/1725 bør sådanne oplysninger typisk ikke betragtes som accessoriske i forbindelse med højrisiko-AI-systemer som omhandlet i bilag III. Hvis AI-systemets output imidlertid kun har ubetydelig eller mindre relevans for menneskelige handlinger eller beslutninger, kan det betragtes som rent accessorisk, herunder f.eks. AI-systemer, der anvendes til oversættelse til informative formål eller dokumentforvaltning.
- (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, race, 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 kritisk digital infrastruktur som opført i punkt 8 i bilag I i direktivet om kritiske enheders modstandsdygtighed, 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. Sikkerhedskomponenter i kritisk infrastruktur, herunder kritisk digital infrastruktur, er systemer, der anvendes til direkte at beskytte den kritiske infrastrukturens fysiske integritet eller menneskers sundhed og sikkerhed og ejendom, men som ikke er nødvendige for, at systemet kan fungere. Svigt eller funktionsfejl i sådanne komponenter kan direkte medføre risici for den kritiske infrastrukturens fysiske integritet og dermed risici for menneskers sundhed og sikkerhed og ejendom. Komponenter, der udelukkende er beregnet til cybersikkerhedsformål, bør ikke betragtes som sikkerhedskomponenter. Eksempler på sikkerhedskomponenter i en sådan kritisk infrastruktur kan omfatte systemer til overvågning af vandtryk eller brandalarmkontrollsystemer i cloudcomputingcentre.
- (35) AI-systemer, der anvendes inden for uddannelse eller erhvervsuddannelse, navnlig til at fastslå adgang, optagelse eller fordeling af personer på uddannelsesinstitutioner eller -programmer på alle niveauer eller til at evaluere personers læringsudbytte, 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 baseret på individuel adfærd eller personlighedstræk eller personlige egenskaber, 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 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 mikrovirksomheder eller små virksomheder som defineret i bilaget til Kommissionens henstilling 2003/361/EF til egen brug. Fysiske personer, der ansøger om eller modtager væsentlige 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, herunder om modtagerne reelt er berettigede til disse ydelser eller tjenester, 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. AI-systemer anvendes også i stigende grad til risikovurdering i forbindelse med fysiske personer og prisfastsættelse i forbindelse med livs- og sygeforsikring, som, hvis den ikke udformes, udvikles og anvendes behørigt, kan have alvorlige konsekvenser for menneskers liv og sundhed, herunder økonomisk udstødelse og forskelsbehandling. For at sikre en konsekvent tilgang inden for sektoren for finansielle tjenesteydelser bør ovennævnte undtagelse for mikrovirksomheder og små virksomheder i forbindelse med egen brug finde anvendelse, for så vidt som de selv leverer og ibrugtager et AI-system med henblik på at sælge deres egne forsikringsprodukter.

- (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 aktiviteters 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, 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. AI-systemer, der specifikt er beregnet til skatte- og toldmyndigheders administrative procedurer og til finansielle efterretningstjenesters udførelse af administrative opgaver, der omfatter analyse af oplysninger i henhold til Unionens lovgivning om bekæmpelse af hvidvask, 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, 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/EU²⁰, Europa-Parlamentets og Rådets forordning (EF) nr. 810/2009²¹ og anden relevant lovgivning.

²⁰ 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).

²¹ 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).

- (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 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 forudindtagethed, fejl og uigennemsigtighed bør de AI-systemer, der har til formål at bistå retlige myndigheder med at 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.
- (41) Klassificeringen af et AI-system som et højrisikosystem i henhold til denne forordning bør ikke fortolkes således, at anvendelsen af systemet 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, medmindre andet specifikt er fastsat i denne forordning.
- (42) For at begrænse risiciene fra højrisiko-AI-systemer, der bringes i omsætning eller på anden måde tages i brug på EU-markedet, 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. Især bør risikostyringssystemet bestå af en kontinuerlig iterativ proces, der er planlagt og løber i hele højrisiko-AI-systemets livscyklus. Denne proces bør sikre, at udbyderen identificerer og analyserer risiciene for sundheden, sikkerheden og de grundlæggende rettigheder for de personer, der kan blive berørt af systemet i lyset af dets tilsigtede formål, herunder de mulige risici som følge af interaktionen mellem AI-systemet og det miljø, som systemet fungerer i, og derfor vedtager passende risikostyringsforanstaltninger i lyset af det aktuelle tekniske niveau.

- (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 prøvningsdatasæt bør være tilstrækkelig relevante og repræsentative og have de tilstrækkelige statistiske egenskaber, herunder med hensyn til de personer eller grupper af personer, på hvilke højrisiko-AI-systemet skal anvendes. Disse datasæt bør også være så fejlfrie og fuldstændige som muligt i lyset af AI-systemets tilsigtede formål, idet der på en forholdsmæssig måde tages hensyn til den tekniske gennemførlighed og det aktuelle tekniske niveau, tilgængeligheden af data og gennemførelsen af passende risikostyringsforanstaltninger, således at eventuelle mangler i datasættene afhjælpes behørigt. Kravet om, at datasættene skal være fuldstændige og fejlfrie, bør ikke påvirke anvendelsen af teknikker til beskyttelse af privatlivets fred i forbindelse med udvikling og prøvning af AI-systemer. Trænings-, validerings- og prøvningsdatasæt bør i det omfang, det er nødvendigt af hensyn til deres tilsigtede formål, tage 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 væsentlig samfundsinteresse, jf. artikel 9, stk. 2, litra g), i forordning (EU) 2016/679 og artikel 10, stk. 2, litra g), i forordning (EU) 2018/1725.

- (44a) Ved anvendelsen af de principper, der er omhandlet i artikel 5, stk. 1, litra c), i forordning (EU) 2016/679 og artikel 4, stk. 1, litra c), i forordning (EU) 2018/1725, navnlig princippet om dataminimering, i forbindelse med trænings-, validerings- og prøvningsdatasæt i henhold til nærværende forordning, bør der tages behørigt hensyn til AI-systemets fulde livscyklus.
- (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. Desuden bør udbydere eller brugere opbevare logfiler, der genereres automatisk af højrisiko-AI-systemet, herunder f.eks. outputdata, startdato og -tidspunkt osv., i det omfang et sådant system og de tilhørende logfiler er under deres kontrol, i en periode, der er passende for, at de kan opfylde deres forpligtelser.

- (47) For at afhjælpe den uigennemsigthed, der kan gøre visse AI-systemer uforståelige eller for komplekse for fysiske personer, bør der kræves en vis grad af gennemsigthed 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 af de personer, der kan blive berørt af systemet i lyset af dets tilsigtede formål, hvis det er relevant. For at gøre det lettere for brugerne at forstå brugsanvisningen bør de indeholde illustrative eksempler, hvor 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. I betragtning af de betydelige konsekvenser for personer i tilfælde af ukorrekte resultater i visse systemer til biometrisk identifikation er det hensigtsmæssigt at fastsætte et skærpet krav om menneskeligt tilsyn for disse systemer, således at brugeren ikke træffer foranstaltninger eller beslutninger på grundlag af den identifikation, der følger af systemet, medmindre den er blevet verificeret og bekræftet særskilt af mindst to fysiske personer. Disse personer kan være fra en eller flere enheder og omfatte den person, der driver eller anvender systemet. Dette krav bør ikke medføre unødvendige byrder eller forsinkelser, og det kan være tilstrækkeligt, at de forskellige personers særskilte verificeringer automatisk registreres i de logfiler, der genereres af systemet.
- (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 i forhold til skadelig eller på anden vis uønsket adfærd, der kan skyldes begrænsninger i systemerne eller det miljø, som systemerne fungerer i, (f.eks. fejl, svigt, uoverensstemmelser og uventede situationer). Højrisiko-AI-systemer bør derfor udformes og udvikles med passende tekniske løsninger for at forebygge eller minimere denne skadelige eller på anden måde uønskede adfærd, f.eks. mekanismer, der gør det muligt for systemet på sikker vis at afbryde dets drift (fejlsikre planer) under tilstedeværelse af visse uregelmæssigheder, eller hvis driften ligger uden for visse forudbestemte grænser. 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 trænede 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. 765/2008²² om kravene til akkreditering og markedsovervågning af produkter, Europa-Parlamentets og Rådets afgørelse nr. 768/2008/EF²³ om fælles rammer for markedsføring af produkter og Europa-Parlamentets og Rådets forordning (EU) 2019/1020²⁴ om markedsovervågning og produktoverensstemmelse ("den nye lovgivningsmæssige ramme for markedsføring af produkter").
- (52a) I overensstemmelse med principperne i den nye lovgivningsmæssige ramme bør der fastsættes specifikke forpligtelser for de relevante operatører i AI-værdikæden for at sikre retssikkerheden og lette overholdelsen af denne forordning. I visse situationer kan disse operatører optræde i mere end én rolle på samme tid og bør derfor kumulativt opfylde alle relevante forpligtelser, der er forbundet med disse roller. F.eks. kan en operatør fungere som distributør og importør på samme tid.
- (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.

²² 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).

²³ 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).

²⁴ 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).

- (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 egen 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.
- (54a) For at sikre retssikkerheden er det nødvendigt at præcisere, at enhver fysisk eller juridisk person under visse særlige omstændigheder bør betragtes som udbyder af et nyt højrisiko-AI-system og derfor bør påtage sig alle de relevante forpligtelser. Dette er f.eks. tilfældet, hvis den person placerer sit navn eller varemærke på et højrisiko-AI-system, der allerede er bragt i omsætning eller taget i brug, eller hvis den person ændrer det tilsigtede formål med et AI-system, der ikke er et højrisikosystem, og som allerede er bragt i omsætning eller taget i brug, på en måde, der gør det ændrede system til et højrisiko-AI-system. Disse bestemmelser bør finde anvendelse med forbehold af mere specifikke bestemmelser, der er fastsat i særlig sektorlovgivning inden for den nye lovgivningsmæssige ramme, som denne forordning bør finde anvendelse sammen med. F.eks. bør artikel 16, stk. 2, i forordning (EU) 2017/745, der fastsætter, at visse ændringer ikke bør betragtes som ændringer af udstyr, der kan påvirke dets opfyldelse af de gældende krav, fortsat finde anvendelse på højrisiko-AI-systemer, der er medicinsk udstyr som omhandlet i nævnte forordning.
- (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 bringes i omsætning eller tages i brug uafhængigt af produktet, bør producenten af produktet 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.
- (56a) For udbydere, der ikke er etableret i Unionen, spiller den autoriserede repræsentant en central rolle med hensyn til at sikre, at højrisiko-AI-systemer, der bringes i omsætning eller tages i brug i Unionen af disse udbydere, overholder kravene, og som fabrikanternes kontaktperson i Unionen. I betragtning af denne centrale rolle og for at sikre, at ansvaret overtages med henblik på håndhævelse af denne forordning, er det hensigtsmæssigt at den bemyndigede repræsentant hæfter solidarisk med udbyderen for defekte højrisiko-AI-systemer. Den autoriserede repræsentants ansvar i henhold til denne forordning berører ikke bestemmelserne i direktiv 85/374/EØF om produktansvar.
- (57) [udgår]
- (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. Disse forpligtelser bør ikke berøre andre brugerforpligtelser i forbindelse med højrisiko-AI-systemer i henhold til EU-retten eller national ret og bør ikke finde anvendelse, hvis anvendelsen sker som led i en personlig ikkeerhvervsmæssig aktivitet.

(58a) Det er hensigtsmæssigt at præcisere, at denne forordning ikke berører de forpligtelser for udbydere og brugere af AI-systemer i deres rolle som dataansvarlige eller databehandlere, der følger af EU-retten om beskyttelse af personoplysninger, for så vidt som udformningen, udviklingen eller anvendelsen af AI-systemer omfatter behandling af personoplysninger. Det er også hensigtsmæssigt at præcisere, at registrerede bevarer alle de rettigheder og garantier, som de har i henhold til EU-retten, herunder rettigheder i forbindelse med udelukkende automatiske individuelle afgørelser, herunder profilering. Harmoniserede regler for omsætning, ibrugtagning og anvendelse af AI-systemer, der er fastsat i henhold til denne forordning, bør lette en effektiv gennemførelse og muliggøre udøvelsen af de registreredes rettigheder og andre retsmidler, der er garanteret i henhold til EU-retten om beskyttelse af personoplysninger og andre grundlæggende rettigheder.

(59) [udgår]

(60) [udgår]

- (61) Standardisering bør spille en central rolle med hensyn til at levere tekniske løsninger til udbydere for at sikre overholdelsen af denne forordning i overensstemmelse med det aktuelle teknologiske niveau. Overholdelse af harmoniserede standarder som defineret i Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012²⁵, der som regel forventes at afspejle det aktuelle teknologiske niveau, bør være et middel for udbydere til at påvise overensstemmelse med kravene i denne forordning. I mangel af relevante referencer til harmoniserede standarder bør Kommissionen dog ved hjælp af gennemførelsesretsakter kunne fastsætte fælles specifikationer for visse krav i henhold til denne forordning som en ekstraordinær fallbackløsning for at lette udbyderens forpligtelse til at opfylde kravene i denne forordning, når standardiseringsprocessen er blokeret, eller når der er forsinkelser i udarbejdelsen af en passende harmoniseret standard. Hvis en sådan forsinkelse skyldes den pågældende standards tekniske kompleksitet, bør Kommissionen overveje dette, inden den overvejer at udarbejde fælles specifikationer. En passende inddragelse af små og mellemstore virksomheder i udarbejdelsen af standarder til støtte for gennemførelsen af denne forordning er afgørende for at fremme innovation og konkurrenceevne inden for kunstig intelligens i Unionen. En sådan inddragelse bør sikres på passende vis i overensstemmelse med artikel 5 og 6 i forordning (EU) nr. 1025/2012.

²⁵ 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).

- (61a) Uden at det berører anvendelsen af harmoniserede standarder og fælles specifikationer, bør udbydere have en formodning om overensstemmelse med det relevante datakrav, når deres højrisiko-AI-system er blevet trænet og prøvet med data, der afspejler de specifikke geografiske, adfærdsmæssige eller funktionelle rammer, som AI-systemet skal anvendes indenfor. Tilsvarende og i overensstemmelse med artikel 54, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2019/881 formodes højrisiko-AI-systemer, der er certificeret, eller for hvilke der er udstedt en overensstemmelseserklæring i henhold til en cybersikkerhedsordning i henhold til nævnte forordning, hvis referencer er offentliggjort i Den Europæiske Unions Tidende, at være i overensstemmelse med cybersikkerhedskravene i nærværende forordning. Dette berører ikke den pågældende cybersikkerhedsordnings frivillige karakter.
- (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 overlapning 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. For så vidt angår højrisiko-AI-systemer i forbindelse med produkter, der er omfattet af forordning (EU) 745/2017 og (EU) 746/2017 om medicinsk udstyr, bør anvendelsen af kravene i denne forordning ikke berøre eller tage hensyn til risikostyringslogikken og vurderingen af fordele og risici inden for rammen for medicinsk udstyr.
- (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 de bemyndigede organer notificeres 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. De nationale kompetente myndigheder bør sende notifikationen af disse organer til Kommissionen og de andre medlemsstater ved hjælp af det elektroniske notifikationsværktøj, der er udviklet og forvaltes af Kommissionen i henhold til artikel R23 i afgørelse nr. 768/2008/EF.
- (66) I overensstemmelse med det almindeligt anerkendte begreb væsentlig ændring for produkter, der er reguleret af EU-harmoniseringslovgivningen, bør AI-systemet, når der sker en ændring, som kan have indflydelse på højrisiko-AI-systemets overensstemmelse med denne forordning (f.eks. ændring af styresystem eller softwarearkitektur), eller hvis systemets tilsigtede formål ændrer sig, betragtes som et nyt AI-system, der bør underkastes en ny overensstemmelsesvurdering. Ændringer af algoritmen og dens ydeevne for 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), bør ikke udgøre en væsentlig ændring, hvis de er fastlagt på forhånd af udbyderen og vurderet på tidspunktet for overensstemmelsesvurderingen.
- (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 sig selv og oplysninger om deres højrisiko-AI-system i en EU-database, der skal oprettes og forvaltes af Kommissionen. Inden anvendelse af et højrisiko-AI-system, der er opført i bilag III, skal brugere af højrisiko-AI-systemer, der er offentlige myndigheder, agenturer eller organer, med undtagelse af retshåndhævende myndigheder, grænsekontrolmyndigheder, indvandringsmyndigheder eller asylmyndigheder, og myndigheder, der er brugere af højrisiko-AI-systemer inden for kritisk infrastruktur, også registrere sig selv i en sådan database og udvælge det system, de påtænker at anvende. Kommissionen bør være dataansvarlig for denne database i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2018/1725²⁶. For at sikre at databasen fungerer efter hensigten, når den tages i brug, bør proceduren for oprettelse af databasen omfatte, at Kommissionen udarbejder funktionsspecifikationer, samt en uafhængig revisionsrapport.

²⁶ 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).

- (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 er indlysende ud fra en rimelig oplyst, opmærksom og velunderrettet fysisk persons synspunkt under hensyntagen til omstændighederne og anvendelsessammenhængen. Ved gennemførelsen af en sådan forpligtelse bør der tages hensyn til egenskaber hos enkeltpersoner, der tilhører sårbare grupper på grund af deres alder eller handicap, i det omfang AI-systemet også har til formål at interagere med disse grupper. Fysiske personer bør desuden underrettes, når de udsættes for systemer, der ved at behandle personernes biometriske data, kan genkende eller udlede de personers følelser eller hensigter eller tildele dem specifikke kategorier. Sådanne specifikke kategorier kan vedrøre aspekter såsom køn, alder, hårfarve, øjenfarve, tatoveringer, personlighedstræk, etnisk oprindelse, personlige præferencer og interesser eller andre aspekter såsom seksuel orientering eller politisk overbevisning. 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. Overholdelse af ovenfor nævnte oplysningskrav bør ikke fortolkes således, at anvendelsen af systemet eller dets output er lovlig i henhold til denne forordning eller anden EU-ret eller ret i medlemsstaterne, og bør ikke berøre andre gennemsigtighedsforpligtelser for brugere af AI-systemer i EU-ret eller national ret. Den bør desuden ikke fortolkes således, at anvendelse af systemet eller dets output hindrer ytringsfriheden eller retten til frihed for kunst og videnskab, der er sikret ved Den Europæiske Unions charter om grundlæggende rettigheder, navnlig når indholdet er en del af et åbenlyst kreativt, satirisk, kunstnerisk eller fiktivt arbejde eller program, med forbehold for passende garantier for tredjemands rettigheder og friheder.

- (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 for kunstig intelligens 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-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), herunder startupvirksomheder. Deltagelsen i den reguleringsmæssige sandkasse for kunstig intelligens bør fokusere på spørgsmål, der skaber retsusikkerhed for udbydere og potentielle udbydere med hensyn til at innovere, eksperimentere med kunstig intelligens i Unionen og bidrage til evidensbaseret lovgivningsmæssig læring. Tilsynet med AI-systemerne i den reguleringsmæssige sandkasse for kunstig intelligens bør derfor omfatte deres udvikling, træning, prøvning og validering, inden systemerne bringes i omsætning eller tages i brug samt begrebet og forekomsten af væsentlige ændringer, der kan kræve en ny overensstemmelsesvurderingsprocedure. Hvor det er relevant, bør de nationale kompetente myndigheder, der opretter reguleringsmæssige sandkasser for kunstig intelligens, samarbejde med andre relevante myndigheder, herunder dem, der fører tilsyn med beskyttelsen af grundlæggende rettigheder, og gøre det muligt at inddrage andre aktører i AI-økosystemet såsom nationale eller europæiske standardiseringsorganisationer, bemyndigede organer, prøvnings- og forsøgsfaciliteter, forsknings- og forsøgslaboratorier, innovationsknudepunkter og relevante interessenter og civilsamfundsorganisationer. 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. Reguleringsmæssige sandkasser for kunstig intelligens, der oprettes i henhold til denne forordning, bør ikke berøre anden lovgivning, der giver mulighed for at oprette andre sandkasser, der har til formål at sikre overholdelse af anden lovgivning end denne forordning. Hvis det er relevant, bør de relevante kompetente myndigheder med ansvar for disse andre reguleringsmæssige sandkasser også overveje fordelene ved at anvende disse sandkasser med henblik på at sikre AI-systemers overensstemmelse med denne forordning. Efter aftale mellem de nationale kompetente myndigheder og deltagerne i den reguleringsmæssige sandkasse for kunstig intelligens kan prøvning under faktiske forhold også gennemføres og overvåges inden for rammerne af den reguleringsmæssige sandkasse for kunstig intelligens.

- (-72a) Denne forordning bør udgøre retsgrundlaget for deltagerne i den reguleringsmæssige sandkasse for kunstig intelligens til at anvende 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, og artikel 9, stk. 2, litra g), i forordning (EU) 2016/679 og artikel 5 og 10 i forordning (EU) 2018/1725, og uden at det berører artikel 4, stk. 2, og artikel 10 i direktiv (EU) 2016/680. Alle andre forpligtelser for databehandlere og rettigheder for registrerede i henhold til forordning (EU) 2016/679, forordning (EU) 2018/1725 og direktiv (EU) 2016/680 finder fortsat anvendelse. Især bør denne forordning ikke udgøre et retsgrundlag, jf. artikel 22, stk. 2, litra b), i forordning (EU) 2016/679 og artikel 24, stk. 2, litra b), i forordning (EU) 2018/1725. 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.
- (72a) For at fremskynde udviklingen og omsætningen af de højrisiko-AI-systemer, der er opført i bilag III, er det vigtigt, at udbydere eller potentielle udbydere af sådanne systemer også kan drage fordel af en særlig ordning for prøvning af disse systemer under faktiske forhold uden at deltage i en reguleringsmæssig sandkasse for kunstig intelligens. I sådanne tilfælde og under hensyntagen til de mulige konsekvenser af en sådan prøvning for enkeltpersoner bør det imidlertid sikres, at forordningen indfører passende og fornødne garantier og betingelser for udbydere eller potentielle udbydere. Sådanne garantier bør bl.a. omfatte anmodning om fysiske personers informerede samtykke til at deltage i prøvninger under faktiske forhold med undtagelse af retshåndhævelse i tilfælde, hvor indhentning af informeret samtykke ville forhindre AI-systemet i at blive prøvet. Registreredes samtykke til at deltage i sådanne prøvninger i henhold til denne forordning adskiller sig fra og berører ikke de registreredes samtykke til behandling af deres personoplysninger i henhold til den relevante databeskyttelseslovgivning.

- (73) For at fremme og beskytte innovation er det vigtigt, at der tages særligt hensyn til SMV-udbyderes 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 SMV-udbyderes 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 udbyderes dokumentation og kommunikationen med operatører, er et sprog, der forstås bredt af det størst mulige antal brugere på tværs af grænserne.
- (73a) For at fremme og beskytte innovation bør AI-on-demand-plattformen og alle relevante EU-finansieringsprogrammer og -projekter såsom programmet for et digitalt Europa og Horisont Europa, der gennemføres af Kommissionen og medlemsstaterne på nationalt plan eller EU-plan, bidrage til at nå målene i denne forordning.
- (74) For at minimere risiciene i gennemførelsen som følge af manglende viden og ekspertise på markedet samt for at gøre det lettere for udbydere, især SMV'er, og bemyndigede organer at opfylde deres forpligtelser i henhold til denne forordning bør navnlig 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.
- (74a) For at sikre proportionalitet i betragtning af nogle operatørers meget beskedne størrelse med hensyn til innovationsomkostninger er det desuden hensigtsmæssigt at fritage mikrovirksomheder fra de dyreste forpligtelser, såsom etablering af et kvalitetsstyringssystem, der vil mindske den administrative byrde og omkostningerne for disse virksomheder uden at påvirke beskyttelsesniveauet og behovet for opfyldelse af kravene til højrisiko-AI-systemer.

- (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 afspejle AI-økosystemets forskellige interesser og bestå af repræsentanter for medlemsstaterne. For at sikre inddragelse af relevante interessenter bør der nedsættes en stående undergruppe til udvalget. Udvalget bør være ansvarligt for en række rådgivningsopgaver såsom udtalelser, henstillinger, rådgivning eller bidrag til vejledning om spørgsmål vedrørende gennemførelsen af denne forordning, herunder med hensyn til håndhævelsesspørgsmål, tekniske specifikationer eller eksisterende standarder, der er relateret til de krav, der er fastsat i denne forordning, samt rådgive og bistå Kommissionen og medlemsstaterne og deres nationale kompetente myndigheder i forbindelse med specifikke spørgsmål vedrørende kunstig intelligens. For at give medlemsstaterne en vis fleksibilitet i udpegelsen af deres repræsentanter i AI-Udvalget kan sådanne repræsentanter være alle personer, som tilhører offentlige enheder, og som bør have de relevante kompetencer og beføjelser til at lette koordinering på nationalt plan og bidrage til udførelsen af udvalgets opgaver. Udvalget bør nedsætte to stående undergrupper for at tilvejebringe en platform for samarbejde og udveksling mellem markedsovervågningsmyndigheder og bemyndigende myndigheder om spørgsmål vedrørende henholdsvis markedsovervågning og bemyndigede organer. Den stående undergruppe for markedsovervågning bør fungere som den administrative samarbejdsgruppe (ADCO) i forbindelse med denne forordning, jf. artikel 30 i forordning (EU) 2019/1020. I overensstemmelse med Kommissionens rolle og opgaver i henhold til artikel 33 i forordning (EU) 2019/1020 bør Kommissionen støtte aktiviteterne i den stående undergruppe for markedsovervågning ved at foretage markedsevalueringer eller -undersøgelser, navnlig med henblik på at identificere aspekter af denne forordning, der kræver specifik og hurtig koordinering mellem markedsovervågningsmyndighederne. Udvalget kan efter behov nedsætte andre stående eller midlertidige undergrupper med henblik på at behandle specifikke spørgsmål. Udvalget bør også, hvor det er relevant, samarbejde med relevante EU-organer, -ekspertgrupper og -netværk, der er aktive inden for rammerne af relevant EU-lovgivning, herunder navnlig dem, der er aktive i henhold til den relevante EU-forordning om data, digitale produkter og tjenester.

- (76a) Kommissionen bør aktivt støtte medlemsstaterne og operatørerne i gennemførelsen og håndhævelsen af denne forordning. I den forbindelse bør den udarbejde retningslinjer om særlige emner med henblik på at lette anvendelsen af denne forordning, samtidig med at der lægges særlig vægt på SMV'ers og startupvirksomheders behov i de sektorer, som med størst sandsynlighed vil blive berørt. For at støtte passende håndhævelse og medlemsstaternes kapaciteter bør der oprettes EU-prøvningsfaciliteter for AI og en pulje af relevante eksperter, som stilles til rådighed for medlemsstaterne.
- (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. Medlemsstaterne kan beslutte at udpege enhver form for offentlig enhed til at udføre de nationale kompetente myndigheders opgaver som defineret i denne forordning i overensstemmelse med deres specifikke nationale organisatoriske karakteristika og behov.
- (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 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. Markedsovervågningsmyndigheder, der er udpeget i henhold til denne forordning, bør alle have håndhævelsesbeføjelser i henhold til denne forordning og forordning (EU) 2019/1020 og bør udøve deres beføjelser og udføre deres opgaver uafhængigt, upartisk og uden bias. Selv om de fleste AI-systemer ikke er underlagt specifikke krav og forpligtelser i henhold til denne forordning, kan markedsovervågningsmyndighederne træffe foranstaltninger vedrørende alle AI-systemer, når de udgør en risiko i henhold til denne forordning. På grund af den særlige karakter af Unionens institutioner, agenturer og organer, der er omfattet af denne forordnings anvendelsesområde, er det hensigtsmæssigt at udpege Den Europæiske Tilsynsførende for Databeskyttelse til en kompetent markedsovervågningsmyndighed for dem. Dette bør ikke berøre medlemsstaternes udpegelse af nationale kompetente myndigheder. Markedsovervågningsaktiviteter bør ikke påvirke de tilsynsbelagte enheders evne til at udføre deres opgaver uafhængigt, når en sådan uafhængighed er påkrævet i henhold til EU-retten.
- (79a) Denne forordning berører ikke kompetencerne, opgaverne, beføjelserne og uafhængigheden for så vidt angår de relevante nationale offentlige myndigheder eller organer, der fører tilsyn med anvendelsen af EU-retten om beskyttelse af grundlæggende rettigheder, herunder ligestillingsorganer og databeskyttelsesmyndigheder. Disse nationale offentlige myndigheder eller organer bør også i det omfang, det er nødvendigt for deres mandat, også have adgang til al den dokumentation, der er udarbejdet i henhold til denne forordning. Der bør fastsættes en særlig beskyttelsesprocedure for at sikre passende og rettidig håndhævelse over for AI-systemer, som udgør en risiko for sundhed, sikkerhed og grundlæggende rettigheder. Proceduren for sådanne AI-systemer, som udgør en risiko, bør anvendes på højrisiko-AI-systemer, der udgør en risiko, forbudte systemer, der er bragt i omsætning, taget i brug eller anvendt i strid med den forbudte praksis, der er fastsat i denne forordning, og AI-systemer, der er gjort tilgængelige i strid med de gennemsigtighedskrav, der er fastsat i denne forordning og udgør en risiko.

- (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, 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, medmindre medlemsstaterne beslutter at udpege en anden myndighed til at udføre disse markedsovervågningsopgaver. Disse kompetente myndigheder bør have alle beføjelser i henhold til denne forordning og forordning (EU) 2019/1020 om markedsovervågning til at håndhæve denne forordnings krav og forpligtelser, herunder beføjelser til at udføre ex post-markedsovervågningsaktiviteter, der, hvor det er relevant, kan integreres i deres eksisterende tilsynsmekanismer og -procedurer i henhold til den relevante EU-lovgivning om finansielle tjenesteydelser. Det bør fastsættes, at de nationale myndigheder, der er ansvarlige for tilsynet med kreditinstitutter, som er reguleret ved direktiv 2013/36/EU, og som deltager i den fælles tilsynsmekanisme (FTM), der er oprettet ved Rådets forordning (EF) nr. 1024/2013, når de fungerer som markedsovervågningsmyndigheder i henhold til denne forordning, straks bør indberette alle oplysninger, som identificeres i forbindelse med deres markedsovervågningsaktiviteter, og som kan være af potentiel interesse for Den Europæiske Centralbanks tilsynsopgaver som fastsat i nævnte forordning, til Den Europæiske Centralbank. 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/EU²⁷, bør nogle af udbydernes proceduremæssige forpligtelser i forbindelse med risikostyring, overvågning efter omsætning og dokumentation indarbejdes i de eksisterende forpligtelser og procedurer i henhold til direktiv 2013/36/EU. For at undgå overlapninger 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. Den samme ordning bør gælde for forsikrings- og genforsikringsselskaber og forsikringsholdingselskaber i henhold til direktiv 2009/138/EU (Solvens II) og

²⁷ 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).

forsikringsformidlere i henhold til direktiv (EU) 2016/97 og andre typer finansielle institutioner, der er underlagt krav vedrørende intern forvaltning, ordninger eller processer, der er fastsat i henhold til den relevante EU-lovgivning om finansielle tjenesteydelser, for at sikre konsekvens og ligebehandling i den finansielle sektor.

- (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 krav, der gælder for højrisiko-AI-systemer, og som er tilpasset i lyset af det tilsigtede formål med systemerne og involverede lavere risici. 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 AI-udvikling 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/EF²⁸ 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 i overensstemmelse med EU-retten eller national ret.

²⁸ 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).

- (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 og med respekt for princippet om *ne bis in idem*. 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 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 lovgivning²⁹. 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. Sådanne høringer og sådan rådgivningsstøtte bør også gennemføres inden for rammerne af AI-Udvalgets og dets undergruppers aktiviteter.

²⁹ EUT L 123 af 12.5.2016, s. 1.

- (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. 182/2011³⁰. Det er navnlig vigtigt, at Kommissionen i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning, når der er behov for bredere ekspertise i den tidlige udarbejdelse af udkast til gennemførelsesretsakter, gør brug af ekspertgrupper, hører udvalgte interessenter eller gennemfører offentlige høringer, hvis det er relevant. Sådanne høringer og sådan rådgivningsstøtte bør også ske inden for rammerne af AI-Udvalgets og dets undergruppers aktiviteter, herunder udarbejdelse af gennemførelsesretsakter i forbindelse med artikel 4, 4b og 6.
- (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.
- (87a) Med henblik på at sikre retssikkerheden, sikre en passende tilpasningsperiode for operatører og undgå markedsforstyrrelser, herunder ved at sikre kontinuitet i anvendelsen af AI-systemer, bør denne forordning kun finde anvendelse på højrisiko-AI-systemer, der er bragt i omsætning eller taget i brug inden den generelle anvendelsesdato, hvis disse systemer fra denne dato er genstand for betydelige ændringer af deres design eller tilsigtede formål. Det er hensigtsmæssigt at præcisere, at begrebet betydelig ændring i denne henseende bør forstås som indholdsmæssigt ækvivalent med begrebet væsentlig ændring, som kun anvendes i forbindelse med højrisiko-AI-systemer som defineret i denne forordning.

³⁰ 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).

- (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 [...] –

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 bestemte AI-systemer
- d) regler om markedsovervågning, markedstilsyn og forvaltning
- e) foranstaltninger til støtte for innovation.

Artikel 2

Anvendelsesområde

1. Denne forordning finder anvendelse på:
 - a) udbydere, der omsætter eller ibrugtager AI-systemer i Unionen, uanset om samme udbydere fysisk befinder sig eller er etableret i Unionen eller i et tredjeland
 - b) brugere af AI-systemer, der fysisk befinder sig eller er etableret i Unionen
 - c) udbydere og brugere af AI-systemer, der fysisk befinder sig eller er etableret i et tredjeland, hvis det output, der produceres af systemet, anvendes i Unionen
 - d) importører og distributører af AI-systemer
 - e) producenter af et produkt, der under eget navn eller varemærke bringer et AI-system i omsætning eller tager det i brug sammen med deres produkt
 - f) bemyndigede repræsentanter for udbydere, der er etableret i Unionen.

2. For så vidt angår AI-systemer, der er klassificeret som højrisiko-AI-systemer i henhold til artikel 6, stk. 1, og artikel 6, stk. 2, i forbindelse med produkter, der er omfattet af EU-harmoniseringslovgivningen i bilag II, afsnit B, finder kun artikel 84 i denne forordning anvendelse. Artikel 53 finder kun anvendelse, for så vidt kravene til højrisiko-AI-systemer i henhold til denne forordning er blevet integreret i den pågældende EU-harmoniseringslovgivning.

3. Denne forordning finder ikke anvendelse på AI-systemer, hvis og i det omfang de bringes i omsætning, tages i brug eller anvendes med eller uden ændring af sådanne systemer med henblik på aktiviteter, der ikke er omfattet af EU-rettens anvendelsesområde, og under alle omstændigheder aktiviteter vedrørende militær, forsvar eller national sikkerhed, uanset hvilken type enhed der udfører disse aktiviteter.

Desuden finder denne forordning ikke anvendelse på AI-systemer, der ikke bringes i omsætning eller tages i brug i Unionen, hvis outputtet anvendes i Unionen til aktiviteter, der falder uden for EU-rettens anvendelsesområde, og under alle omstændigheder aktiviteter vedrørende militær, forsvar eller national sikkerhed, uanset hvilken type enhed der udfører disse aktiviteter.

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 4, i Europa-Parlamentets og Rådets direktiv 2000/31/EF³¹ [*skal erstattes af de tilsvarende bestemmelser i retsakten om digitale tjenester*].
6. Denne forordning finder ikke anvendelse på AI-systemer, herunder deres output, som specifikt er udviklet og taget i brug udelukkende med henblik på videnskabelig forskning og udvikling.
7. Denne forordning finder ikke anvendelse på forsknings- og udviklingsaktiviteter vedrørende AI-systemer.
8. Denne forordning finder ikke anvendelse på forpligtelser for brugere, som er fysiske personer, der anvender AI-systemer som led i rent personlige ikkeerhvervsmæssige aktiviteter, undtagen artikel 52.

³¹ 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).

Artikel 3

Definitioner

I denne forordning forstås ved:

- 1) "system med kunstig intelligens" (AI-system): et system, som er udformet med henblik på at fungere med elementer af autonomi, og som på grundlag af data og input fra maskiner og/eller mennesker udleder, hvordan et givet sæt mål kan nås ved hjælp af maskinlæring og/eller logiske og videnbaserede tilgange, og som producerer systemgenereret output såsom indhold (generative AI-systemer), forudsigelser, anbefalinger eller beslutninger, der påvirker de miljøer, som AI-systemet interagerer med
- 1a) "et AI-systems livscyklus": et AI-systems levetid fra udformning til afvikling. Uden at det berører markedsovervågningsmyndighedernes beføjelser, kan en sådan afvikling ske på et hvilket som helst tidspunkt i fasen med overvågning efter omsætning ved en beslutning truffet af udbyderen og indebærer, at systemet ikke må anvendes længere. Et AI-systems livscyklus afsluttes også ved en væsentlig ændring af AI-systemet foretaget af udbyderen eller en anden fysisk eller juridisk person, i hvilket tilfælde det væsentligt ændrede AI-system betragtes som et nyt AI-system
- 1b) "AI-system til generelle formål": et AI-system, der – uanset hvordan det bringes i omsætning eller tages i brug, herunder som open source software – efter udbyderens hensigt skal udføre generelt anvendelige funktioner såsom billed- og talegenkendelse, generering af lyd og video, mønstergenkendelse, besvarelse af spørgsmål, oversættelse og andre funktioner; et AI-system til generelle formål kan anvendes i mange forskellige sammenhænge og integreres i mange forskellige andre AI-systemer
- 2) "udbyder": en fysisk eller juridisk person, en offentlig myndighed, et agentur eller et andet organ, der udvikler eller får udviklet et AI-system og bringer det i omsætning eller tager det i brug under eget navn eller varemærke, enten mod betaling eller gratis

- 3) [udgår]
- 3a) "små og mellemstore virksomheder" (SMV'er): virksomheder i henhold til definitionen i bilaget til Kommissionens henstilling 2003/361/EF om definitionen af mikrovirksomheder, små og mellemstore virksomheder
- 4) "bruger": enhver fysisk eller juridisk person, herunder en offentlig myndighed eller ethvert agentur eller andet organ, under hvis myndighed systemet anvendes
- 5) "bemyndiget repræsentant": enhver fysisk eller juridisk person, der fysisk befinder sig eller er etableret i Unionen, og som har modtaget og accepteret 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
- 5a) "producent af et produkt": producent i henhold til den EU-harmoniseringslovgivning, der er anført i bilag II
- 6) "importør": enhver fysisk eller juridisk person, som fysisk befinder sig eller er etableret i Unionen, og som bringer et AI-system i omsætning, 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
- 8) "operatør": udbyderen, producenten af et produkt, brugeren, den bemyndigede repræsentant, importøren eller distributøren
- 9) "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 i Unionen 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
- 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 eller tages ud af drift eller deaktiveres
- 17) "tilbagetrækning af et AI-system": enhver foranstaltning, der har til formål at forhindre, at et AI-system i forsyningskæden gøres tilgængeligt på markedet
- 18) "et AI-systems ydeevne": et AI-systems evne til at opfylde det tilsigtede formål
- 19) "overensstemmelsesvurdering": en proces til verificering af, om de i afsnit III, kapitel 2, i denne forordning fastsatte krav vedrørende et højrisiko-AI-system er opfyldt

- 20) "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
- 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 en ændring af det tilsigtede formål, med hensyn til hvilket AI-systemet er vurderet. 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
- 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, eller i artikel 4b i denne forordning fastsatte krav og anden gældende EU-retsakt om harmonisering af betingelser for omsætning af produkter ("EU-harmoniseringslovgivning") og om anbringelse af denne mærkning
- 25) "system til overvågning efter omsætningen": alle aktiviteter, som udbydere af AI-systemer udfører for 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 specifikation": et sæt af teknisk specifikationer som defineret i artikel 2, nr. 4), i forordning (EU) nr. 1025/2012, der giver mulighed for at opfylde visse krav, 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
- 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 som f.eks. ansigtsbilleder eller fingeraftryksoplysninger
- 34) "system til følelsesgenkendelse": et AI-system, der har til formål at genkende eller udlede fysiske personers psykiske tilstand, 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 på grundlag af deres biometriske data

- 36) "system til biometrisk fjernidentifikation": et AI-system, der har til formål at identificere fysiske personer typisk på afstand, uden deres aktive deltagelse, ved at sammenligne en persons biometriske data med de biometriske data i en referencedatabase
- 37) "system til biometrisk fjernidentifikation i realtid": et system til biometrisk fjernidentifikation, hvor optagelse af biometriske data, sammenligning og identifikation finder sted øjeblikkeligt eller næsten øjeblikkeligt
- 38) [udgår]
- 39) "offentlige steder": ethvert offentligt eller privatejet fysisk sted, der er tilgængeligt for et ubestemt antal fysiske personer, uanset om visse betingelser eller omstændigheder for adgang er fastlagt på forhånd, og uanset de potentielle kapacitetsbegrænsninger
- 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 udføres af retshåndhævende myndigheder eller på deres vegne, 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) [udgår]

- 43) "national kompetent myndighed": enhver af følgende: den bemyndigende myndighed og markedsovervågningsmyndigheden. For så vidt angår AI-systemer, der tages i brug eller anvendes af EU-institutioner, -agenturer, -kontorer og -organer, varetager Den Europæiske Tilsynsførende for Databeskyttelse de ansvarsområder, som i medlemsstaterne er overdraget til den nationale kompetente myndighed, og, hvor det er relevant, forstås enhver henvisning til nationale kompetente myndigheder eller markedsovervågningsmyndigheder i denne forordning som en henvisning til Den Europæiske Tilsynsførende for Databeskyttelse
- 44) "alvorlig hændelse": enhver hændelse eller funktionsfejl i et AI-system, som direkte eller indirekte fører til et af følgende udfald:
- a) et menneskes død eller alvorlig skade på et menneskes helbred
 - b) en alvorlig og uoprettelig forstyrrelse i forvaltningen og driften af kritisk infrastruktur
 - c) misligholdelse af forpligtelser i henhold til den del af EU-retten, der har til formål at beskytte de grundlæggende rettigheder
 - d) alvorlig skade på ejendom eller miljøet.
- 45) "kritisk infrastruktur": et aktiv, et system eller en del heraf, der er nødvendig for at levere en tjenesteydelse af uundværlig betydning for at opretholde vitale samfundsmæssige funktioner eller økonomiske aktiviteter som omhandlet i artikel 2, stk. 4 og 5, i direktiv/..... om kritiske enheders modstandsdygtighed
- 46) "personoplysninger": oplysninger som defineret i artikel 4, nr. 1), i forordning (EU) 2016/679
- 47) "andre data end personoplysninger": andre data end personoplysninger som defineret i artikel 4, nr. 1), i forordning (EU) 2016/679

- 48) "prøvning under faktiske forhold": midlertidig prøvning af et AI-system med henblik på dets tilsigtede formål under faktiske forhold uden for et laboratorium eller på anden måde simuleret miljø med henblik på at indsamle pålidelige og solide data og vurdere og verificere AI-systemets overensstemmelse med kravene i denne forordning; prøvning under faktiske forhold anses ikke for at bringe AI-systemet i omsætning eller tage det i brug i henhold til denne forordning, forudsat at alle betingelser i henhold til artikel 53 eller artikel 54a er opfyldt
- 49) "plan for prøvning under faktiske forhold": et dokument, der beskriver mål, metode, geografisk, befolkningsmæssig og tidsmæssig rækkevidde, overvågning, tilrettelæggelse og gennemførelse af prøvning under faktiske forhold
- 50) "forsøgsperson" med henblik på prøvning under faktiske forhold: en fysisk person, der deltager i prøvninger under faktiske forhold
- 51) "informeret samtykke": en forsøgspersons frie og frivillige tilkendegivelse af sin vilje til at deltage i en bestemt prøvning under faktiske forhold efter at være blevet informeret om alle aspekter af prøvningen, der er relevante for forsøgspersonens beslutning om at deltage; når der er tale om mindreårige og forsøgspersoner uden handleevne gives det informerede samtykke af deres retligt udpegede repræsentant
- 52) "reguleringsmæssig sandkasse for kunstig intelligens": en konkret ramme, som er oprettet af en national kompetent myndighed, og som giver udbydere eller potentielle udbydere af AI-systemer mulighed for at udvikle, uddanne, validere og prøve, hvor det er relevant under faktiske forhold, et innovativt AI-system i henhold til en specifik plan for en begrænset periode under reguleringsmæssigt tilsyn.

Artikel 4
Gennemførelsesretsakter

For at sikre ensartede betingelser for gennemførelsen af denne forordning for så vidt angår maskinlæringstilgange og logiske og videnbaserede tilgange, jf. artikel 3, stk. 1, kan Kommissionen vedtage gennemførelsesretsakter for at præcisere de tekniske elementer i disse tilgange under hensyntagen til den markeds-mæssige og teknologiske udvikling. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 74, stk. 2.

AFSNIT IA

AI-SYSTEMER TIL GENERELLE FORMÅL

Artikel 4a

Overholdelse af denne forordning for så vidt angår AI-systemer til generelle formål

1. Uden at det berører denne forordnings artikel 5, 52, 53 og 69, skal AI-systemer til generelle formål kun opfylde de krav og forpligtelser, der er fastsat i artikel 4b.
2. Sådanne krav og forpligtelser finder anvendelse, uanset om AI-systemet til generelle formål bringes i omsætning eller tages i brug som en forhåndstrænet model, og om yderligere finjustering af modellen skal udføres af brugeren af AI-systemet til generelle formål.

Artikel 4b

Krav til AI-systemer til generelle formål og forpligtelser for udbydere af sådanne systemer

1. AI-systemer til generelle formål, der kan anvendes som højrisiko-AI-systemer eller som komponenter i højrisiko-AI-systemer, jf. artikel 6, skal opfylde kravene i afsnit III, kapitel 2, i denne forordning fra anvendelsesdatoen for de gennemførelsesretsakter, som Kommissionen vedtager efter undersøgelsesproceduren i artikel 74, stk. 2, senest 18 måneder efter denne forordnings ikrafttræden. Disse gennemførelsesretsakter angiver og tilpasser anvendelsen af kravene i afsnit III, kapitel 2, til AI-systemer til generelle formål på baggrund af deres karakteristika, tekniske gennemførlighed, særlige forhold i AI-værdikæden og den markedsmæssige og teknologiske udvikling. Ved opfyldelsen af disse krav tages der hensyn til det generelt anerkendte tekniske niveau.
2. Udbydere af AI-systemer til generelle formål, jf. stk. 1, skal fra anvendelsesdatoen for de gennemførelsesretsakter, jf. stk. 1, opfylde forpligtelserne i artikel 16aa, 16e, 16f, 16 g, 16i, 16j, 25, 48 og 61.
3. Med henblik på at opfylde forpligtelserne i artikel 16e skal udbyderne følge den overensstemmelsesvurderingsprocedure, der er baseret på intern kontrol, jf. bilag VI, punkt 3 og 4.
4. Udbydere af sådanne systemer opbevarer også den tekniske dokumentation, jf. artikel 11, så den står til rådighed for de nationale kompetente myndigheder i en periode, der slutter ti år, efter at AI-systemet til generelle formål bringes i omsætning eller tages i brug i Unionen.

5. Udbydere af AI-systemer til generelle formål samarbejder med og giver de nødvendige oplysninger til andre udbydere, der har til hensigt at ibrugtage eller bringe sådanne systemer i omsætning på EU-markedet som højrisiko-AI-systemer eller som komponenter i højrisiko-AI-systemer, med henblik på at sætte sidstnævnte i stand til at opfylde deres forpligtelser i henhold til denne forordning. Et sådant samarbejde mellem udbydere bevarer, hvor det er relevant, intellektuelle ejendomsrettigheder og fortrolige forretningsoplysninger eller forretningshemmeligheder i overensstemmelse med artikel 70. For at sikre ensartede betingelser for gennemførelsen af denne forordning for så vidt angår de oplysninger, som udbydere af AI-systemer til generelle formål skal dele, kan Kommissionen vedtage gennemførelsesretsakter efter den undersøgelsesprocedure, der er omhandlet i artikel 74, stk. 2.
6. Ved opfyldelse af de krav og forpligtelser, der er omhandlet i stk. 1, 2 og 3:
- enhver henvisning til det tilsigtede formål skal forstås som en henvisning til en eventuel anvendelse af AI-systemer til generelle formål som højrisiko-AI-systemer eller som komponenter i højrisiko-AI-systemer, jf. artikel 6
 - enhver henvisning til kravene til højrisiko-AI-systemer i kapitel II, afsnit III, skal forstås således, at den kun henviser til kravene i nærværende artikel.

Artikel 4c

Undtagelser til artikel 4b

1. Artikel 4b finder ikke anvendelse, når udbyderen udtrykkeligt har udelukket alle højrisikoanvendelser i brugsanvisningen eller de oplysninger, der ledsager AI-systemet til generelle formål.
2. En sådan udelukkelse foretages i god tro og anses ikke for berettiget, hvis udbyderen har tilstrækkelige grunde til at antage, at systemet kan misbruges.
3. Når udbyderen opdager eller underrettes om markedsmisbrug, træffer vedkommende alle nødvendige og forholdsmæssige foranstaltninger for at forhindre et sådant yderligere misbrug, navnlig under hensyntagen til omfanget af misbruget og alvoren af de dermed forbundne risici.

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 eller med det resultat i væsentlig grad at fordreje en persons adfærd på en måde, der påfører eller med rimelighed 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, handicap eller en særlig social eller økonomisk situation med henblik på eller med det resultat i væsentlig grad at fordreje en til gruppen hørende persons adfærd på en måde, der påfører eller med rimelighed vil påføre den pågældende person eller en anden person fysisk eller psykisk skade
 - c) omsætning, ibrugtagning eller anvendelse af AI-systemer med henblik på evaluering eller klassificering af fysiske personers 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 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 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 af retshåndhævende myndigheder eller på deres vegne 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
 - ii) forebyggelse af en specifik og væsentlig trussel mod kritisk infrastruktur, fysiske personers liv, sundhed eller fysiske sikkerhed eller forebyggelse af terrorangreb
 - iii) lokalisering eller identifikation af en fysisk person med henblik på at efterforske, retsforfølge eller fuldbyrde strafferetlige sanktioner for strafbare handlinger, der er omhandlet i artikel 2, stk. 2, i Rådets rammeafgørelse 2002/584/JHA³², og som i den pågældende medlemsstat kan straffes med frihedsstraf eller en anden frihedsberøvende foranstaltning af en maksimal varighed på mindst tre år, eller andre specifikke strafbare handlinger, som i den pågældende medlemsstat kan straffes med frihedsstraf eller en anden frihedsberøvende foranstaltning af en maksimal varighed på mindst fem 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

³² Rådets rammeafgørelse 2002/584/RIA af 13. juni 2002 om den europæiske arrestordre og om procedurene for overgivelse mellem medlemsstaterne (EFT L 190 af 18.7.2002, s. 1).

- 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 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 på betingelse af, at der anmodes om en sådan tilladelse uden unødigt forsinkelse under anvendelsen af AI-systemet, og hvis en sådan tilladelse afvises, bringes systemets anvendelse straks til ophør.

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 og indberetning 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

HØJRIKOS-AI-SYSTEMER

KAPITEL 1

KLASSIFICERING AF AI-SYSTEMER SOM HØJRIKOSYSTEMER

Artikel 6

Klassificeringsregler for højrisiko-AI-systemer

1. Et AI-system, som i sig selv er et produkt, der er omfattet af den EU-harmoniseringslovgivning, der er anført i bilag II, betragtes som et højrisikosystem, hvis det skal underkastes en overensstemmelsesvurdering foretaget af en tredjepart med henblik på omsætning eller ibrugtagning af produktet i henhold til ovennævnte lovgivning.

2. Et AI-system, der er beregnet til at blive anvendt som en sikkerhedskomponent i et produkt, der er omfattet af den i stk. 1 omhandlede lovgivning, betragtes som et højrisikosystem, hvis det skal underkastes en overensstemmelsesvurdering foretaget af en tredjepart med henblik på omsætning eller ibrugtagning af produktet i henhold til ovennævnte lovgivning. Denne bestemmelse finder anvendelse, uanset om AI-systemet bringes i omsætning eller tages i brug uafhængigt af produktet.
3. AI-systemer, der er omhandlet i bilag III, betragtes som højrisikosystemer, medmindre systemets output er rent accessorisk i forhold til den relevante foranstaltning eller afgørelse, der skal træffes, og medfører sandsynligvis derfor ikke til en væsentlig risiko for sundheden, sikkerheden eller de grundlæggende rettigheder.

For at sikre ensartede betingelser for gennemførelsen af denne forordning vedtager Kommissionen senest et år efter denne forordnings ikrafttræden gennemførelsesretsakter for at præcisere de omstændigheder, hvor AI-systemers output som omhandlet i bilag III ville være rent accessorisk med hensyn til den relevante foranstaltning eller afgørelse, der skal træffes. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 74, stk. 2.

Artikel 7

Ændring af bilag III

1. Kommissionen tillægges beføjelse til at vedtage delegerede retsakter, jf. artikel 73, med henblik på at ændre 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, ikke 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
 - i) omfanget af og sandsynligheden for fordele ved anvendelsen af kunstig intelligens for enkeltpersoner, grupper eller samfundet som helhed.
3. Kommissionen tillægges beføjelse til at vedtage delegerede retsakter, jf. artikel 73, med henblik på at ændre listen i bilag III ved at fjerne højrisiko-AI-systemer, hvis begge følgende betingelser er opfyldt:
- a) det eller de pågældende højrisiko-AI-system(er) udgør ikke længere nogen væsentlig risiko for de grundlæggende rettigheder, sundheden eller sikkerheden under hensyntagen til kriterierne i stk. 2
 - b) fjernelsen reducerer ikke det generelle beskyttelsesniveau for sundhed, sikkerhed og grundlæggende rettigheder i henhold til EU-retten.

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, under hensyntagen til det generelt anerkendte aktuelle teknologiske niveau.

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 skal forstås som en kontinuerlig iterativ proces, der er planlagt og 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, der med størst sandsynlighed vil opstå for sundhed, sikkerhed og grundlæggende rettigheder i lyset af højrisiko-AI-systemets tilsigtede formål
 - b) [udgår]
 - 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.

De i dette stykke omhandlede risici vedrører kun dem, der med rimelighed kan afbødes eller fjernes gennem udviklingen eller udformningen af højrisiko-AI-systemet eller tilvejebringelsen af tilstrækkelige tekniske oplysninger.

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 med henblik på at minimere risiciene mere effektivt og samtidig opnå en passende balance i gennemførelsen af foranstaltningerne til opfyldelse af disse krav.
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.

I fastlæggelsen af de mest hensigtsmæssige risikostyringsforanstaltninger sikres følgende:

- a) fjernelse eller i videst mulig omfang begrænsning af de risici, der er identificeret og evalueret i henhold til stk. 2, så vidt muligt gennem passende udformning og udvikling af højrisiko-AI-systemet
- 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.

Med henblik på 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 sikre, at højrisiko-AI-systemer fungerer på en måde, der er i overensstemmelse med deres tilsigtede formål og opfylder de krav, der er fastsat i dette kapitel.
6. Prøvningsprocedurerne kan omfatte prøvning under faktiske forhold i henhold til artikel 54a.

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 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 personer under 18 år.
9. For udbydere af højrisiko-AI-systemer, der er underlagt krav vedrørende interne risikostyringsprocesser i henhold til relevant sektorspecifik EU-ret, kan de aspekter, der er beskrevet i stk. 1-8, være en del af de risikostyringsprocedurer, der er fastlagt i henhold til denne ret.

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) dataindsamlingsprocesser
 - 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 forudindtagethed, der må forventes at påvirke fysiske personers sundhed og sikkerhed eller føre til forskelsbehandling, som er forbudt i henhold til EU-retten
 - g) kortlægning af eventuelle datamangler eller datautilstrækkeligheder, og hvordan de kan afhjælpes.
3. Trænings-, validerings- og prøvningsdatasæt er relevante, repræsentative og i videst muligt omfang fejlfrie 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 forudindtagethed 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. Ved udvikling af højrisiko-AI-systemer, der ikke gør brug af teknikker, der omfatter træning af modeller, finder stk. 2-5 kun anvendelse på prøvningsdatasættene.

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 på en klar og forståelig måde til de nationale kompetente myndigheder og bemyndigede organer.

Dokumentationen skal som minimum indeholde de i bilag IV fastsatte elementer, eller, i tilfælde af SMV'er, herunder startupvirksomheder, enhver tilsvarende dokumentation, der indfrier samme mål, medmindre den kompetente myndighed anser dem for at være uhensigtsmæssige.

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 skal teknisk gøre det muligt, at hændelser ("logfiler") registreres automatisk i løbet af systemets livscyklus.
2. For at sikre en passende grad af sporbarhed i AI-systemet i forhold til systemets tilsigtede formål skal logningen gøre det muligt at registrere hændelser, der er relevante for:
 - i) identifikation af situationer, der kan medføre, at et AI-system udgør en risiko, jf. artikel 65, stk. 1, eller en væsentlig ændring
 - ii) lettelse af overvågningen efter omsætningen, jf. artikel 61 og
 - iii) overvågning af driften af højrisiko-AI-systemer, jf. artikel 29, stk. 4.
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 opfylde de relevante bruger- og udbyderforpligtelser, der er fastsat i dette afsnits kapitel 3, og sætte brugerne i stand til at forstå og anvende systemet korrekt.
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, herunder de specifikke geografiske, adfærdsmæssige eller funktionelle rammer, inden for hvilke højrisiko-AI-systemet skal anvendes
 - ii) det niveau af nøjagtighed, herunder systemets parametre, robusthed og cybersikkerhed, jf. artikel 15, i forhold til hvilket højrisiko-AI-systemet er prøvet 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, der med rimelighed kan forudses, kan medføre risici for menneskers sundhed og sikkerhed eller grundlæggende rettigheder, jf. artikel 9, stk. 2

- iv) hvis det er relevant, systemets adfærd for så vidt angår de specifikke 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
 - vi) hvis det er relevant, en beskrivelse af systemets forventede output
- 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) de nødvendige beregnings- og hardwareressourcer, højrisiko-AI-systemets forventede levetid og eventuelle nødvendige vedligeholdelses- og plejeforanstaltninger, herunder deres hyppighed, for at sikre, at AI-systemet fungerer korrekt, herunder med hensyn til softwareopdateringer
 - f) en beskrivelse af mekanismen, der er medtaget i AI-systemet, og som giver brugerne mulighed for på korrekt vis at indsamle, lagre og fortolke logfilerne, hvis det er relevant.

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 typer foranstaltninger:
 - a) foranstaltninger, der 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) foranstaltninger, der 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. Med henblik på gennemførelsen af stk. 1-3 leveres højrisiko-AI-systemet til brugeren på en sådan måde, at det er muligt for fysiske personer, der foretager menneskeligt tilsyn, når det er relevant og forholdsmæssigt efter omstændighederne, at:
 - a) forstå højrisiko-AI-systemets kapacitet og begrænsninger og være i stand til at overvåge dets drift på behørig vis
 - b) være opmærksomme på den mulige tendens til automatisk eller i overdreven grad af forlade sig på output fra højrisiko-AI-systemet ("automatiseringspartiskhed")
 - c) fortolke højrisiko-AI-systemets output korrekt under hensyntagen til f. eks. de tilgængelige fortolkningsværktøjer og -metoder
 - d) 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) 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 særskilt af mindst to fysiske personer. Kravet om en særskilt verifikation foretaget af mindst to fysiske personer finder ikke anvendelse på højrisiko-AI-systemer, der anvendes med henblik på retshåndhævelse, migrationsstyring, grænsekontrol og asylforvaltning, i tilfælde, hvor anvendelsen af dette krav efter EU-retten eller national ret er uforholdsmæssig.

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.

Højrisiko-AI-systemers robusthed kan opnås ved hjælp af tekniske redundansløsninger, som kan omfatte backupplaner eller fejlsikre planer.

De højrisiko-AI-systemer, der fortsætter med at lære efter at være bragt i omsætning eller taget i brug, udvikles på en sådan måde for i videst mulig omfang at fjerne eller reducere risikoen for indvirkning af eventuelle partiske output på input i fremtidig drift ("feedbacksløjfer") og behørigt imødegås ved hjælp af passende afbødende foranstaltninger.

4. 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

FORPLIGTELSE 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
- aa) angive deres navn, registrerede firmanavn eller registrerede varemærke og kontaktadresse 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
- b) indføre et kvalitetsstyringssystem, der er i overensstemmelse med artikel 17
- c) opbevare dokumentation, jf. artikel 18

- d) opbevare de logfiler, der automatisk genereres af deres højrisiko-AI-systemer, når logfilerne er under deres kontrol, jf. artikel 20
- e) sørge for, at højrisiko-AI-systemet underkastes den relevante overensstemmelsesvurderingsprocedure, jf. artikel 43, inden systemet bringes i omsætning eller tages i brug
- f) opfylde registreringsforpligtelsen, jf. artikel 51, stk. 1
- g) træffe de nødvendige korrigerende foranstaltninger, jf. artikel 21, hvis højrisiko-AI-systemet ikke er i overensstemmelse med de krav, der er fastsat i dette afsnits kapitel 2
- h) underrette den relevante nationale kompetente myndighed 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 en alvorlig hændelse, 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.
- 2a. For de udbydere af højrisiko-AI-systemer, der er underlagt forpligtelser vedrørende kvalitetssikringssystemer i henhold til relevant sektorspecifik EU-ret, kan de aspekter, der er beskrevet i stk. 1, være en del af kvalitetsstyringssystemerne i henhold til denne ret.
3. For de udbydere, der er finansielle institutioner, der er underlagt krav vedrørende deres interne ledelse, ordninger eller processer i henhold til EU-lovgivningen om finansielle tjenesteydelser, anses forpligtelsen til at indføre et kvalitetsstyringssystem med undtagelse af stk. 1, litra g), h) og i), for at være opfyldt ved overholdelse af reglerne om ordninger eller procedurer for intern ledelse i henhold til den relevante EU-lovgivning om finansielle tjenesteydelser. I den forbindelse tages der hensyn til alle de harmoniserede standarder, der er nævnt i artikel 40 i denne forordning.

Artikel 18

Opbevaring af dokumentation

1. 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.
- 1a. Hver medlemsstat fastsætter, på hvilke betingelser den i stk. 1 omhandlede dokumentation fortsat står til rådighed for de nationale kompetente myndigheder i den periode, der er anført i nævnte stykke, i de tilfælde, hvor en udbyder eller dennes bemyndigede repræsentant, der er etableret på dens område, går konkurs eller indstiller sine aktiviteter inden udløbet af denne periode.
2. De udbydere, der er finansielle institutioner, som er underlagt krav vedrørende deres interne ledelse, ordninger eller processer i henhold til EU-lovgivningen om finansielle tjenesteydelser, vedligeholder den tekniske dokumentation som en del af dokumentationen, der opbevares i henhold til den relevante EU-lovgivning om finansielle tjenesteydelser.

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. [udgår]

Artikel 20

Automatisk genererede logfiler

1. Udbydere af højrisiko-AI-systemer opbevarer de logfiler, jf. artikel 12, stk. 1, 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. De opbevarer dem i en periode på mindst seks måneder, medmindre andet er fastsat i gældende EU-ret eller national ret, navnlig EU-retten om beskyttelse af personoplysninger.
2. De udbydere, som er finansielle institutioner, som er underlagt krav vedrørende deres interne ledelse, ordninger eller processer i henhold til EU-lovgivningen om finansielle tjenesteydelser, opbevarer de logfiler, der automatisk genereres af deres højrisiko-AI-systemer som en del af dokumentationen, der opbevares i henhold til den relevante lovgivning om finansielle tjenesteydelser.

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, undersøger straks, hvis det er relevant, årsagerne i samarbejde med den indberettende bruger og træffer 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 sprog, som den pågældende myndighed let kan forstå. Efter begrundet anmodning fra en national kompetent myndighed giver udbydere også denne myndighed adgang til de logfiler, jf. artikel 12, stk. 1, 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 23a
Betingelser for, at andre personer er omfattet af en udbyders forpligtelser

1. Enhver fysisk eller juridisk person anses for at være udbyder af et nyt højrisiko-AI-system med henblik på denne forordning og er underlagt forpligtelserne for udbydere, jf. artikel 16, i følgende tilfælde:
 - a) de sætter deres navn eller varemærke på et højrisiko-AI-system, der allerede er bragt i omsætning eller taget i brug, med forbehold af kontraktbestemmelser om, at forpligtelserne er fordelt anderledes

- b) [udgår]
 - c) de foretager en væsentlig ændring af et højrisiko-AI-system, der allerede er bragt i omsætning eller taget i brug
 - d) de ændrer det tilsigtede formål med et AI-system, der ikke er et højrisikosystem, og som allerede er bragt i omsætning eller taget i brug, på en måde der gør det ændrede system til et højrisiko-AI-system
 - e) de bringer et AI-system til generelle formål i omsætning eller tager det i brug som et højrisiko-AI-system eller som en komponent i et højrisiko-AI-system.
2. Hvis de omstændigheder, der er omhandlet i stk. 1, litra a) eller c), indtræffer, anses den udbyder, der oprindeligt bragte højrisiko-AI-systemet i omsætning eller tog det i brug, ikke længere for at være en udbyder i denne forordnings forstand.
3. For højrisiko-AI-systemer, der er sikkerhedskomponenter i produkter, der er omfattet af retsakterne opført i bilag II, afsnit A, anses producenten af disse produkter for at være udbyderen af højrisiko-AI-systemet og underlægges forpligtelserne i henhold til artikel 16 i et af følgende scenarier:
- i) højrisiko-AI-systemet bringes i omsætning sammen med produktet under producentens navn eller varemærke
 - ii) højrisiko-AI-systemet tages i brug under producentens navn eller varemærke, efter at produktet er bragt i omsætning.

Artikel 24

[udgår]

Artikel 25

Bemyndigede repræsentanter

1. Udbydere, der er etableret uden for Unionen, skal 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. Med henblik på denne forordning skal fuldmagten sætte den bemyndigede repræsentant i stand til at udføre følgende opgaver:
 - a) at kontrollere, at EU-overensstemmelseserklæringen og den tekniske dokumentation er blevet udarbejdet, og at en passende overensstemmelsesvurderingsprocedure er blevet gennemført af udbyderen
 - a) i en periode, der udløber 10 år efter, at højrisiko-AI-systemet er blevet bragt i omsætning eller taget i brug, at kunne forelægge de nationale kompetente myndigheder og nationale myndigheder, der er omhandlet i artikel 63, stk. 7, kontaktoplysningerne for den udbyder, som den bemyndigede repræsentant er udpeget af, en kopi af EU-overensstemmelseserklæringen, den tekniske dokumentation og, hvis det er relevant, den attest, der er udstedt af det bemyndigede organ
 - b) efter begrundet anmodning at give de nationale kompetente myndigheder alle de oplysninger og al den dokumentation, herunder den, som opbevares i henhold til litra b), 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, jf. artikel 12, stk. 1, 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.

- d) at opfylde registreringsforpligtelsen, jf. artikel 51, stk. 1, og, hvis registreringen af systemet foretages af udbyderen selv, kontrollere, at de oplysninger, der er omhandlet i bilag VIII, del II, 1-11, er korrekte.

Den bemyndigede repræsentant bringer fuldmagten til ophør, hvis vedkommende har tilstrækkelige grunde til at antage, at udbyderen handler i strid med sine forpligtelser i henhold til denne forordning. I så fald underretter den straks markedsovervågningsmyndigheden i den medlemsstat, hvor den er etableret, samt, hvor det er relevant, det relevante bemyndigede organ om mandatets ophør og begrundelsen herfor.

Den bemyndigede repræsentant er retligt ansvarlig for defekte AI-systemer på samme grundlag som og hæfter solidarisk med udbyderen for så vidt angår dennes potentielle ansvar i henhold til Rådets direktiv 85/374/EØF.

Artikel 26

Forpligtelser for importører

1. Importører af højrisiko-AI-systemer skal, før de bringer sådanne systemer i omsætning, sikre, at et sådant system er i overensstemmelse med denne forordning, ved at kontrollere, at:
 - a) udbyderen af dette AI-system har gennemført den relevante overensstemmelsesvurderingsprocedure, jf. artikel 43
 - b) udbyderen har udarbejdet den tekniske dokumentation i overensstemmelse med bilag IV
 - c) systemet er forsynet med den krævede CE-overensstemmelsesmærkning og er ledsaget af den krævede EU-overensstemmelseserklæring og brugsanvisning.
 - d) udbyderen har udpeget den i artikel 25 omhandlede bemyndigede repræsentant.

2. Hvis en importør har tilstrækkelig begrundelse til at formode, at et højrisiko-AI-system ikke er i overensstemmelse med denne forordning eller er forfalsket eller ledsaget af forfalsket dokumentation, 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, den bemyndigede repræsentant 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.
- 4a. Importøren skal i 10 år efter, at AI-systemet er blevet bragt i omsætning eller taget i brug, opbevare en kopi af den attest, der er udstedt af det bemyndigede organ, hvor det er relevant, af brugsanvisningen og af EU-overensstemmelseserklæringen.
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, herunder den, der opbevares i overensstemmelse med stk. 5, der kræves for at påvise, at et højrisiko-AI-system er i overensstemmelse med kravene i dette afsnits kapitel 2. Med henblik herpå skal de også sikre, at den tekniske dokumentation kan stilles til rådighed for disse myndigheder.
- 5a. Importører samarbejder med de nationale kompetente myndigheder om enhver foranstaltning, som disse myndigheder træffer i forbindelse med et AI-system, som de er importør af.

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 en kopi af EU-overensstemmelseserklæringen og brugsanvisning, og at udbyderen og importøren af systemet, alt efter hvad der er relevant, har opfyldt deres forpligtelser i henholdsvis artikel 16, litra b) og artikel 26, stk. 4.
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 oplysninger og al dokumentation vedrørende dens aktiviteter som beskrevet i stk. 1-4.
- 5a. Distributørerne skal samarbejde med nationale kompetente myndigheder om enhver foranstaltning, der træffes vedrørende et AI-system, som de er distributør af.

Artikel 28

[udgår]

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. denne artikels stk. 2 og 5.
- 1a. Brugere skal tildele menneskeligt tilsyn til fysiske personer, der har den nødvendige kompetence, uddannelse og myndighed.
2. Forpligtelserne i stk. 1 og 1a 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. Brugere skal gennemføre menneskeligt tilsyn og 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 og afbryde anvendelsen af AI-systemet. Hvis brugeren ikke er i stand til at kontakte udbyderen, finder artikel 62 tilsvarende anvendelse. Denne forpligtelse omfatter ikke følsomme operationelle data om brugere af AI-systemer, som er retshåndhævende myndigheder.

For brugere, der er finansielle institutioner, der er underlagt krav vedrørende deres interne ledelse, ordninger eller processer i henhold til EU-lovgivningen om finansielle tjenesteydelser, anses overvågningsforpligtelsen i første afsnit for at være opfyldt ved overholdelse af reglerne om ordninger, procedurer og mekanismer for intern ledelse i henhold til den relevante lovgivning om finansielle tjenesteydelser.

5. Brugere af højrisiko-AI-systemer skal opbevare de logfiler, jf. artikel 12, stk. 1, der genereres automatisk af det pågældende højrisiko-AI-system, i det omfang sådanne logfiler er under deres kontrol. De opbevarer dem i en periode på mindst seks måneder, medmindre andet er fastsat i gældende EU-ret eller national ret, navnlig EU-retten om beskyttelse af personoplysninger.

Brugere, der er finansielle institutioner, som er underlagt krav vedrørende deres interne ledelse, ordninger eller processer i henhold til EU-lovgivningen om finansielle tjenesteydelser, skal opbevare logfilerne som en del af dokumentationen, der opbevares i henhold til den relevante EU-lovgivning om finansielle tjenesteydelser.

- 5a. Brugere af højrisiko-AI-systemer, der er offentlige myndigheder, agenturer eller organer, med undtagelse af retshåndhævende myndigheder, grænsekontrolmyndigheder, indvandringsmyndigheder eller asylmyndigheder, skal opfylde de registreringsforpligtelser, der er omhandlet i artikel 51. Hvis de konstaterer, at det system, de påtænker at anvende, ikke er registreret i den EU-database, der er omhandlet i artikel 60, må de ikke anvende dette system og skal underrette leverandøren eller distributøren.

6. 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.
- 6a. Brugere skal samarbejde med nationale kompetente myndigheder om enhver foranstaltning, der træffes vedrørende et AI-system, som de er bruger af.

KAPITEL 4

BEMYNDIGENDE MYNDIGHEDER OG BEMYNDIGEDE ORGANER

Artikel 30

Bemyndigende myndigheder

1. Hver medlemsstat skal udpege eller oprette mindst 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 beslutte, at den i stk. 1 omhandlede vurdering og overvågning skal foretages af et nationalt akkrediteringsorgan som defineret i og i overensstemmelse med forordning (EF) nr. 765/2008.
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 i overensstemmelse med artikel 70.
7. Bemyndigende myndigheder skal have et tilstrækkelig stort kompetent personale til, at de kan udføre deres opgaver behørigt.
8. [udgår]

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-systemer, 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 akkrediteringscertificat, skal det forelægge den bemyndigende myndighed al 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. Det bemyndigede organ ajourfører den i stk. 2 og stk. 3 omhandlede dokumentation, når der opstår relevante ændringer, for at give myndigheden med ansvar for bemyndigede organer mulighed for at overvåge og kontrollere, at alle krav i artikel 33 fortsat overholdes.

Artikel 32

Bemyndigelsesprocedure

1. De bemyndigende myndigheder må kun bemyndige overensstemmelsesvurderingsorganer, som opfylder kravene i artikel 33.
2. De bemyndigende myndigheder notificerer disse organer til Kommissionen og de øvrige medlemsstater ved hjælp af det elektroniske notifikationsværktøj, der er udviklet og forvaltes af Kommissionen.
3. Bemyndigelsen som omhandlet i stk. 2 skal indeholde fyldestgørende oplysninger om overensstemmelsesvurderingsaktiviteterne, det eller de pågældende overensstemmelsesvurderingsmoduler og AI-systemer og den relevante dokumentation for kompetencen. Hvis en bemyndigelse ikke er baseret på et akkrediteringscertifikat som omhandlet i artikel 31, stk. 2, skal den bemyndigende myndighed forelægge Kommissionen og de øvrige medlemsstater den dokumentation, der attesterer overensstemmelsesvurderingsorganets kompetence, og oplysninger om de ordninger, der er indført til sikring af, at der regelmæssigt føres tilsyn med organet, og at organet også for fremtiden vil opfylde de i artikel 33 fastsatte krav.

4. Det pågældende overensstemmelsesvurderingsorgan må kun udføre aktiviteter som bemyndiget organ, hvis Kommissionen og de øvrige medlemsstater ikke har gjort indsigelse inden for to uger efter en bemyndigelse, der er baseret på et akkrediteringscertifikat, jf. artikel 31, stk. 2, eller senest to måneder efter bemyndigelsen, hvis den indeholder den dokumentation, der er omhandlet i artikel 31, stk. 3.
5. [udgår]

Artikel 33

Krav vedrørende bemyndigede organer

1. Et bemyndiget organ skal oprettes i henhold til national lovgivning og være en juridisk person.
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 højrisiko-AI-systemet, 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 i overensstemmelse med artikel 70, 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, hvor de er beliggende, er ansvarlig i henhold til national ret, eller medlemsstaten selv 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. Det bemyndigede organ skal 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, juridisk 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. [udgår]

Artikel 33a

Formodning om overensstemmelse med krav vedrørende bemyndigede organer

Hvis et overensstemmelsesvurderingsorgan dokumenterer, at det opfylder kriterierne i de relevante harmoniserede standarder eller dele heraf, hvortil der er offentliggjort en reference i Den Europæiske Unions Tidende, formodes det at opfylde kravene i artikel 33, for så vidt som de gældende harmoniserede standarder dækker disse krav.

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 relevante dokumenter vedrørende vurderingen af underentreprenørens eller dattervirksomhedens kvalifikationer og det arbejde, som de har udført i henhold til denne forordning, stilles til rådighed for den bemyndigende myndighed i en periode på 5 år fra datoen for afslutningen af underentrepriseaktiviteten.

Artikel 34a

Bemyndigede organers operationelle forpligtelser

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 udføre deres aktiviteter, idet de undgår unødvendige byrder for udbyderne og under behørig hensyntagen til en virksomheds størrelse, til den sektor, som den opererer inden for, til dens struktur og til, hvor kompleks det pågældende højrisiko-AI-system er. I denne forbindelse skal det bemyndigede organ dog respektere den grad af strenghed og det beskyttelsesniveau, der kræves for, at højrisiko-AI-systemet er i overensstemmelse med kravene i denne forordning.
3. 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 denne myndighed kan udføre sine vurderings-, udpegelses-, bemyndigelses- og tilsynsaktiviteter og fremme vurderingen som anført i dette kapitel.

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. Den bemyndigende myndighed underretter Kommissionen og de øvrige medlemsstater om alle relevante ændringer i notifikationen af et bemyndiget organ via det elektroniske notifikationsværktøj, der er omhandlet i artikel 32, stk. 2.
2. Procedurerne i artikel 31 og artikel 32 finder anvendelse på udvidelser af rammerne for notifikationen. Med hensyn til andre ændringer af notifikationen end udvidelser af rammerne for den, finder procedurerne i de følgende stykker anvendelse.

Hvis et bemyndiget organ beslutter at indstille sine overensstemmelsesvurderingsaktiviteter, underretter det den bemyndigende myndighed og udbyderne hurtigst muligt og i tilfælde af planlagt indstilling ét år, inden dets aktiviteter indstilles. Attesterne kan forblive gyldige i en midlertidig periode på ni måneder, efter at det bemyndigede organs aktiviteter er indstillet, forudsat at et andet bemyndiget organ skriftligt har bekræftet, at det vil påtage sig ansvaret for de AI-systemer, der er omfattet af disse attester. Det nye bemyndigede organ foretager en fuld vurdering af de berørte AI-systemer inden udgangen af denne periode, før det udsteder nye attester for disse systemer. Hvis det bemyndigede organ har indstillet sine aktiviteter, inddrager den bemyndigende myndighed udpegelsen.

3. Hvis en bemyndigende myndighed har tilstrækkelige grunde til at antage, at et bemyndiget organ ikke længere opfylder kravene i artikel 33, eller at det ikke opfylder sine forpligtelser, skal den bemyndigende myndighed, forudsat at det bemyndigede organ har haft mulighed for at fremføre sine synspunkter, begrænse, suspendere eller inddrage bemyndigelsen, alt efter hvad der er mest hensigtsmæssigt, alt efter i hvor alvorlig grad organet ikke opfylder disse krav eller forpligtelser. Den skal straks underrette Kommissionen og de øvrige medlemsstater herom.
4. Hvis et bemyndiget organs udpegelse er blevet suspenderet, begrænset eller helt eller delvist inddraget, underretter dette organ de pågældende fabrikanter inden for senest ti dage.
5. Hvis en bemyndigelse begrænses, suspenderes eller inddrages, skal den bemyndigende myndighed træffe de nødvendige foranstaltninger for at sikre, at det pågældende bemyndigede organs sager opbevares, og stille dem til rådighed for bemyndigende myndigheder i andre medlemsstater og for markedsovervågningsmyndighederne efter disses anmodning.
6. Hvis en udpegelse begrænses, suspenderes eller inddrages, skal den bemyndigende myndighed:
 - a) vurdere indvirkningen på attester, der er udstedt af det bemyndigede organ
 - b) forelægge en rapport om sine resultater til Kommissionen og de øvrige medlemsstater senest tre måneder efter, at den har givet meddelelse om ændringerne af bemyndigelsen
 - c) pålægge det bemyndigede organ at suspendere eller inddrage alle attester, der uretmæssigt er blevet udstedt, inden for en rimelig tidsfrist, der fastsættes af myndigheden, for at sikre AI-systemers overensstemmelse på markedet
 - d) underrette Kommissionen og medlemsstaterne om attester, som den har krævet suspenderet eller tilbagekaldt

- e) give de nationale kompetente myndigheder i den medlemsstat, hvor udbyderen har sit registrerede forretningssted, alle relevante oplysninger om de attester, for hvilke den har krævet suspension eller tilbagekaldelse. Den kompetente myndighed træffer de fornødne foranstaltninger, hvis det er nødvendigt, for at undgå en potentiel risiko for sundhed, sikkerhed eller grundlæggende rettigheder.

7. Med undtagelse af uretmæssigt udstedte attester og tilfælde, hvor en bemyndigelse er blevet inddraget eller begrænset, vedbliver attesterne med at være gyldige i følgende tilfælde:

- a) den bemyndigende myndighed har senest én måned efter suspensionen eller begrænsningen bekræftet, at der ikke er nogen risiko for sundhed, sikkerhed eller grundlæggende rettigheder vedrørende attester, der er berørt af suspensionen eller begrænsningen, og den bemyndigende myndighed har angivet en frist og forventede foranstaltninger til at afhjælpe suspensionen eller begrænsningen, eller
- b) den bemyndigende myndighed har bekræftet, at ingen attester af relevans for suspensionen vil blive udstedt, ændret eller genudstedt under suspensionen eller begrænsningen, og anfører, hvorvidt det bemyndigede organ har kapacitet til at fortsætte overvågningen og fortsat være ansvarligt for eksisterende udstedte attester i suspensions- eller begrænsningsperioden. Hvis myndigheden med ansvar for bemyndigede organer fastslår, at det bemyndigede organ ikke er i stand til at støtte eksisterende udstedte attester, skal udbyderen senest tre måneder efter suspensionen eller begrænsningen skriftligt bekræfte over for de nationale kompetente myndigheder i den medlemsstat, hvor udbyderen af det system, der er omfattet af attesten, har sit registrerede forretningssted, at et andet kvalificeret bemyndiget organ midlertidigt varetager det bemyndigede organs funktioner med hensyn til at overvåge og forblive ansvarligt for attesterne i suspensions- eller begrænsningsperioden.

8. Med undtagelse af uretmæssigt udstedte attester og tilfælde, hvor en udpegelse er blevet inddraget, vedbliver attesterne med at være gyldige i følgende tilfælde:

- a) hvis den nationale kompetente myndighed i den medlemsstat, hvor udbyderen af det AI-system, der er omfattet af attesten, har sit registrerede forretningssted, har bekræftet, at der ikke er nogen risiko for sundhed, sikkerhed og grundlæggende rettigheder i forbindelse med de pågældende systemer, og
- b) et andet bemyndiget organ skriftligt har bekræftet, at det straks varetager ansvaret for disse systemer og vil have færdiggjort vurderingen af det inden 12 måneder efter inddragelsen af udpegelsen.

Under de omstændigheder, der er omhandlet i stk. 1, kan den kompetente nationale myndighed i den medlemsstat, hvor udbyderen af det system, der er omfattet af attesten, har sit forretningssted, forlænge attesternes foreløbige gyldighed i yderligere perioder på tre måneder, dog i alt højst 12 måneder.

Den kompetente nationale myndighed eller det bemyndigede organ, der varetager funktionerne for det bemyndigede organ, der er berørt af ændringen af bemyndigelsen, underretter straks Kommissionen, de øvrige medlemsstater og de øvrige bemyndigede organer herom.

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 i overensstemmelse med artikel 70.

4. Hvis Kommissionen konstaterer, at et bemyndiget organ ikke eller ikke længere opfylder kravene i artikel 33, underretter den den bemyndigende medlemsstat myndighed om begrundelsen for en sådan konstatering og anmoder den om at træffe de nødvendige korrigerende foranstaltninger, herunder om nødvendigt suspension, begrænsning eller inddragelse af bemyndigelsen. Hvis den bemyndigende myndighed ikke træffer de nødvendige foranstaltninger, kan Kommissionen ved hjælp af gennemførelsesretsakter suspendere, begrænse eller inddrage bemyndigelsen. Denne gennemførelsesretsakt vedtages efter undersøgelsesproceduren, jf. artikel 74, stk. 2.

Artikel 38

Koordinering af bemyndigede organer

1. Kommissionen sikrer, at der med hensyn til højrisiko-AI-systemer etableres passende koordinering og samarbejde mellem de bemyndigede organer, der er aktive inden for overensstemmelsesvurderingsprocedurer i henhold til denne forordning, og at det i form af en sektorspecifik gruppe af bemyndigede organer fungerer korrekt.
2. Den bemyndigende myndighed 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, forudsat at de opfylder kravene i artikel 33.

KAPITEL 5

STANDARDER, OVERENSSTEMMELSESVURDERING, CERTIFIKATER, REGISTRERING

Artikel 40

Harmoniserede standarder

1. Højrisiko-AI-systemer eller AI-systemer til generelle formål, 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, eller, hvis det er relevant, med kravene i artikel 4a og artikel 4b for så vidt de nævnte standarder omfatter disse krav.
2. Når Kommissionen udsteder en standardiseringsanmodning til europæiske standardiseringsorganisationer i overensstemmelse med artikel 10 i forordning nr. 1025/2012, præciserer den, at standarderne er sammenhængende, klare og udformet på en sådan måde, at de navnlig har til formål at opfylde følgende mål:
 - a) garantere, at AI-systemer, der bringes i omsætning eller tages i brug i Unionen, er sikre og respekterer Unionens værdier og styrker Unionens åbne strategiske autonomi
 - b) fremme investeringer og innovation inden for AI, herunder gennem øget retssikkerhed, samt konkurrenceevne og vækst på EU-markedet
 - c) styrke forvaltningsstrukturer, der involverer mange interessenter og er repræsentative for alle relevante europæiske interessenter (f.eks. industrien, SMV'er, civilsamfundet, forskere)
 - d) bidrage til at styrke et globalt samarbejde om standardisering inden for kunstig intelligens, der er i overensstemmelse med Unionens værdier og interesser.

Kommissionen anmoder de europæiske standardiseringsorganisationer om at dokumentere deres bedste indsats for at nå ovennævnte mål.

Artikel 41
Fælles specifikationer

1. Kommissionen tillægges beføjelser til efter høring af AI-Udvalget, jf. artikel 56, at vedtage gennemførelsesretsakter efter undersøgelsesproceduren i artikel 74, stk. 2, om fastlæggelse af fælles tekniske specifikationer for kravene i dette afsnits kapitel 2 eller, hvis det er relevant, med kravene i artikel 4a og artikel 4b, hvis følgende betingelser er opfyldt:
 - a) Ingen henvisning til harmoniserede standarder, der dækker de relevante væsentlige hensyn til sikkerhed eller grundlæggende rettigheder, offentliggøres i Den Europæiske Unions Tidende i overensstemmelse med forordning (EU) nr. 1025/2012
 - b) Kommissionen har i henhold til artikel 10, stk. 1, i forordning (EF) nr. 1025/2012 anmodet en eller flere europæiske standardiseringsorganisationer om at udarbejde en harmoniseret standard for de krav, der er fastsat i kapitel 2 i dette afsnit
 - c) den anmodning, der er omhandlet i litra b), ikke er blevet accepteret af nogen af de europæiske standardiseringsorganisationer, eller de harmoniserede standarder, der behandler anmodningen, ikke leveres inden for den frist, der er fastsat i overensstemmelse med artikel 10, stk. 1, i forordning (EF) nr. 1025/2012, eller disse standarder ikke er i overensstemmelse med anmodningen.
- 1a. Inden Kommissionen udarbejder et udkast til gennemførelsesretsakt, underretter den det udvalg, der er omhandlet i artikel 22 i forordning (EU) nr. 1025/2012, om, at den anser betingelserne i stk. 1 for opfyldt.
2. Under den tidlige udarbejdelse af udkastet til gennemførelsesretsakt om den fælles specifikation opfylder Kommissionen de mål, der er omhandlet i artikel 40, stk. 2, og indhenter synspunkter fra relevante organer eller ekspertgrupper, der er nedsat i henhold til relevant sektorspecifik EU-ret. På grundlag af denne høring udarbejder Kommissionen udkastet til gennemførelsesretsakt.

3. Højrisiko-AI-systemer eller AI-systemer til generelle formål, 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, eller, hvis det er relevant, med kravene i artikel 4a og artikel 4b, for så vidt de nævnte fælles specifikationer omfatter disse krav.
4. Når referencer til en harmoniseret standard offentliggøres i Den Europæiske Unions Tidende, ophæves de gennemførelsesretsakter, der er omhandlet i stk. 1, og som omfatter de krav, der er fastsat i dette afsnits kapitel 2, eller kravene i artikel 4a og artikel 4b, alt efter hvad der er relevant.
5. Hvis en medlemsstat finder, at en fælles specifikation ikke fuldt ud opfylder kravene i dette afsnits kapitel 2 eller kravene i artikel 4a og artikel 4b, alt efter hvad der er relevant, underretter den Kommissionen herom med en detaljeret redegørelse, og Kommissionen vurderer disse oplysninger og ændrer, hvis det er relevant, gennemførelsesretsakten om fastlæggelse af den pågældende fælles specifikation.

Artikel 42

Formodning om overensstemmelse med visse krav

1. Højrisiko-AI-systemer, der er blevet trænet og prøvet med data, som afspejler de specifikke geografiske, adfærdsmæssige eller funktionelle rammer, som de skal anvendes inden for, at opfylde de respektive krav i artikel 10, stk. 4.

2. Højrisiko-AI-systemer eller AI-systemer til generelle formål, 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) 2019/881³³, 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, vælge en af følgende procedurer:
- a) overensstemmelsesvurderingsproceduren på grundlag af intern kontrol som omhandlet i bilag VI eller
 - 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.

³³ 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).

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, 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 højrisko-AI-systemer, der er omhandlet i bilag III, punkt 2-8, og AI-systemer til generelle formål skal udbyderne følge overensstemmelsesvurderingsproceduren på grundlag af intern kontrol som omhandlet i bilag VI, som ikke foreskriver inddragelse af et bemyndiget organ.
3. For højrisko-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 højrisko-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 højrisko-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. [udgår]

5. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 73 for at ajourføre bilag VI og bilag VII 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, udfærdiges på et sprog, som er letforståeligt for de relevante myndigheder i den medlemsstat, hvor det bemyndigede organ er etableret.
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. Et eventuelt tillæg til en attest er gyldigt lige så længe som den attest, det supplerer.
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

De bemyndigede organers afgørelser skal kunne appelleres.

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-systemer, relevante oplysninger om spørgsmål vedrørende negative og, efter anmodning, positive overensstemmelsesvurderingsresultater.
- 4. Forpligtelserne i stk. 1-3 skal opfyldes i overensstemmelse med artikel 70.

Artikel 47

Undtagelse fra overensstemmelsesvurderingsprocedure

- 1. Uanset artikel 43 og efter behørigt begrundet anmodning 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, under hensyntagen til de ekstraordinære hensyn, der begrundet undtagelsen. Gennemførelsen af disse procedurer skal ske uden unødigt forsinkelse.
- 1a. I behørigt begrundede hastetilfælde af ekstraordinære hensyn til den offentlige sikkerhed eller i tilfælde af en specifik, væsentlig og overhængende fare for fysiske personers liv eller fysiske sikkerhed kan de retshåndhævende myndigheder eller civilbeskyttelsesmyndighederne tage et specifikt højrisiko-AI-system i brug uden den tilladelse, der er omhandlet i stk. 1, forudsat at der anmodes om en sådan tilladelse under eller efter anvendelsen uden unødigt forsinkelse, og hvis en sådan tilladelse afvises, skal dets anvendelse indstilles med øjeblikkelig virkning, og alle resultater og output af denne anvendelse skal straks kasseres.

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. Denne forpligtelse omfatter ikke følsomme operationelle oplysninger i forbindelse med de retshåndhævende myndigheders aktiviteter.
3. [udgår]
4. [udgår]
5. [udgår]
6. For højrisiko-AI-systemer vedrørende produkter, der er omfattet af EU-harmoniseringslovgivningen, jf. bilag II, afsnit A, finder kun de undtagelsesprocedurer for overensstemmelsesvurdering, der er fastsat i denne lovgivning, anvendelse.

Artikel 48

EU-overensstemmelseserklæring

1. Udbyderen skal udarbejde en skriftlig eller elektronisk undertegnet 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 indgives 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 et sprog, der let kan forstås af de nationale kompetente myndigheder i 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-overensstemmelsesmærkningen er underlagt de generelle principper fastsat i artikel 30 i forordning (EF) nr. 765/2008.
2. 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.
3. Hvor det er relevant, skal CE-mærkningen følges af identifikationsnummeret for det bemyndigede organ, der er ansvarligt for overensstemmelsesvurderingsprocedurerne i artikel 43. Identifikationsnummeret skal også fremgå af salgsfremmende materiale, som nævner, at højrisiko-AI-systemet opfylder kravene til CE-mærkning.

Artikel 50

[udgår]

Artikel 51

Registrering af relevante operatører og højrisiko-AI-systemer i bilag III

1. Inden et højrisiko-AI-system, der er opført i bilag III, med undtagelse af de højrisiko-AI-systemer, der er omhandlet i bilag III, punkt 1, 6 og 7, bringes i omsætning eller tages i brug inden for retshåndhævelse, migration, asyl og grænsekontrol, og højrisiko-AI-systemer som omhandlet i bilag III, punkt 2, registrerer udbyderen og, hvis det er relevant, den bemyndigede repræsentant sig selv i den EU-database, der er omhandlet i artikel 60. Udbyderen eller, hvis det er relevant, den bemyndigede repræsentant registrerer også deres systemer i denne database.
2. Inden anvendelsen af et højrisiko-AI-system, der er opført i bilag III, skal brugere af højrisiko-AI-systemer, som er offentlige myndigheder, agenturer eller organer, eller enheder, der handler på deres vegne, lade sig registrere i den EU-database, der er omhandlet i artikel 60, og udvælge det system, de påtænker at anvende.

Forpligtelserne i foregående afsnit finder ikke anvendelse på retshåndhævende myndigheder, grænsekontrolmyndigheder, indvandringsmyndigheder eller asylmyndigheder, agenturer eller myndigheder, agenturer eller organer, agenturer eller organer, der anvender højrisiko-AI-systemer som omhandlet i bilag III, punkt 2, eller på enheder, der handler på deres vegne.

AFSNIT IV

GENNEMSIGTIGHEDSFORPLIGTELSE FOR UDBYDERE OG BRUGERE AF VISSE AI-SYSTEMER

Artikel 52

Gennemsigtighedsforpligtelser for udbydere og brugere af 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 en rimeligt velinformeret, opmærksom og forsigtig fysisk persons synspunkt 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, med forbehold for passende garantier for tredjemands rettigheder og friheder, medmindre disse systemer er tilgængelige for offentligheden med henblik på at anmelde strafbare handlinger.
2. Brugere af 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, med forbehold for passende garantier for tredjemands rettigheder og frihedsrettigheder.
- 2a. Brugere af et system til følelsesgenkendelse 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 følelsesgenkendelse, og som i henhold til lovgivningen er godkendt til at afsløre, forebygge og efterforske strafbare handlinger, med forbehold for passende garantier for tredjemands rettigheder og frihedsrettigheder.

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 indholdet er en del af et åbenbart kreativt, satirisk, kunstnerisk eller fiktivt arbejde eller program, med forbehold for passende garantier for tredjemands rettigheder og friheder.

- 3a. De oplysninger, der er omhandlet i stk. 1-3, gives til fysiske personer på en klar og synlig måde senest på tidspunktet for den første interaktion eller eksponering.
4. Stk. 1, 2, 2a, 3 og 3a berører ikke kravene og forpligtelserne i nærværende forordnings afsnit III og berører ikke andre gennemsigtighedsforpligtelser for brugere af AI-systemer i EU-ret eller national ret.

AFSNIT V

FORANSTALTNINGER TIL STØTTE FOR INNOVATION

Artikel 53

Reguleringsmæssige sandkasser for kunstig intelligens

- 1a. De nationale kompetente myndigheder kan oprette reguleringsmæssige sandkasser for kunstig intelligens til udvikling, uddannelse, prøvning og validering af innovative AI-systemer under direkte tilsyn, vejledning og støtte fra den nationale kompetente myndighed, inden disse systemer bringes i omsætning eller tages i brug. Sådanne reguleringsmæssige sandkasser kan omfatte prøvning under faktiske forhold under tilsyn af de nationale kompetente myndigheder.

- 1b. [udgår]
 - 1c. Hvor det er relevant, samarbejder de nationale kompetente myndigheder med andre relevante myndigheder og kan gøre det muligt at inddrage andre aktører i AI-økosystemet.
 - 1d. Denne artikel berører ikke andre reguleringsmæssige sandkasser, der er oprettet i henhold til national ret eller EU-ret, herunder i tilfælde, hvor de produkter eller tjenesteydelser, der prøves i dem, er forbundet med anvendelsen af innovative AI-systemer. Medlemsstaterne sikrer et passende samarbejde mellem de myndigheder, der fører tilsyn med disse andre sandkasser, og de nationale kompetente myndigheder.
- 1. [udgår]
 - 1a. [udgår]
 - 1b. Oprettelsen af reguleringsmæssige sandkasser for kunstig intelligens i henhold til nærværende forordning har til formål at bidrage til et eller flere af følgende mål:
 - a) at fremme innovation og konkurrenceevne og lette udviklingen af et AI-økosystem
 - b) at lette og fremskynde adgangen til EU-markedet for AI-systemer, navnlig når de leveres af små og mellemstore virksomheder (SMV'er), herunder startupvirksomheder
 - c) at forbedre retssikkerheden og bidrage til udveksling af bedste praksis gennem samarbejde med de myndigheder, der er involveret i den reguleringsmæssige sandkasse for kunstig intelligens, med henblik på at sikre fremtidig overholdelse af nærværende forordning og, hvis det er relevant, af anden EU-lovgivning og anden lovgivning i medlemsstaterne
 - d) at bidrage til evidensbaseret lovgivningsmæssig læring.
 - 2. [udgår]

- 2a. Adgang til de reguleringsmæssige sandkasser for kunstig intelligens er åben for enhver udbyder eller potentiel udbyder af et AI-system, som opfylder de støtteberettigelses- og udvælgelseskriterier, der er omhandlet i stk. 6, litra a), og som er blevet udvalgt af de nationale kompetente myndigheder efter den udvælgelsesprocedure, der er omhandlet i stk. 6, litra b). Udbydere eller potentielle udbydere kan også indgive ansøgninger i partnerskab med brugere eller andre relevante tredjeparter.

Deltagelse i den reguleringsmæssige sandkasse for kunstig intelligens begrænses til en periode, der er passende i forhold til projektets kompleksitet og omfang. Denne periode kan forlænges af den nationale kompetente myndighed.

Deltagelse i den reguleringsmæssige sandkasse for kunstig intelligens baseres på en specifik plan som omhandlet i denne artikels stk. 6, som aftales mellem deltagerne og den eller de nationale kompetente myndigheder, alt efter hvad der er relevant.

3. Deltagelsen i de reguleringsmæssige sandkasser for kunstig intelligens berører ikke de tilsynsbeføjelser og korrigerende beføjelser, som de myndigheder, der fører tilsyn med sandkassen, har. Disse myndigheder udøver deres tilsynsbeføjelser på en fleksibel måde inden for rammerne af den relevante lovgivning og anvender deres skønsmæssige beføjelser, når de gennemfører retlige bestemmelser for et specifikt projekt vedrørende sandkasser for kunstig intelligens, med det formål at støtte innovation inden for kunstig intelligens i Unionen.

Forudsat at deltageren eller deltagerne overholder sandkasseplanen og vilkårene og betingelserne for deres deltagelse som omhandlet i stk. 6, litra c), og i god tro følger myndighedernes vejledning, pålægger myndighederne ingen administrative bøder for overtrædelse af gældende lovgivning i EU eller medlemsstaterne vedrørende det AI-system, der overvåges i sandkassen, herunder bestemmelserne i nærværende forordning.

4. Deltagerne forbliver ansvarlige i henhold til gældende lovgivning i EU og medlemsstaterne om erstatningsansvar for skader, der forvoldes i forbindelse med deres deltagelse i en reguleringsmæssig sandkasse for kunstig intelligens.

- 4a. Efter anmodning fra udbyderen eller den potentielle udbyder af AI-systemet forelægger den nationale kompetente myndighed, hvis det er relevant, en skriftlig dokumentation for de aktiviteter, der er udført med succes i sandkassen. Den nationale kompetente myndighed forelægger også en slutrapport med en detaljeret beskrivelse af de aktiviteter, der er gennemført i sandkassen, og de dermed forbundne resultater og læringsresultater. Markedsovervågningsmyndighederne eller bemyndigede organer kan, alt efter hvad der er relevant, tage hensyn til en sådan skriftlig dokumentation og slutrapport i forbindelse med overensstemmelsesvurderingsprocedurer eller markedstilsyns kontrol.

Med forbehold af fortrolighedsbestemmelserne i artikel 70 og med samtykke fra sandkassens deltagere har Europa-Kommissionen og AI-Udvalget tilladelse til at få adgang til slutrapporterne og tager, hvis det er relevant, hensyn hertil, når de udfører deres opgaver i henhold til nærværende forordning. Hvis både deltageren og den nationale kompetente myndighed udtrykkeligt accepterer dette, kan slutrapporten gøres offentligt tilgængelig via den centrale informationsplatform, der er omhandlet i artikel 55, stk. 3, litra b).

- 4b. De reguleringsmæssige sandkasser for kunstig intelligens udformes og gennemføres på en sådan måde, at de om relevant letter det grænseoverskridende samarbejde mellem de nationale kompetente myndigheder.
5. De nationale kompetente myndigheder offentliggør årlige rapporter om gennemførelsen af de reguleringsmæssige sandkasser for kunstig intelligens, herunder god praksis, indhøstede erfaringer og anbefalinger vedrørende deres oprettelse og, hvor det er relevant, om anvendelsen af nærværende forordning og anden EU-lovgivning, som der føres tilsyn med inden for sandkassen. Disse årlige rapporter forelægges for AI-Udvalget, som offentliggør et sammendrag af alle eksempler på god praksis, indhøstede erfaringer og anbefalinger. Denne forpligtelse til at gøre årsrapporter offentligt tilgængelige omfatter ikke følsomme operationelle oplysninger i forbindelse med aktiviteter, der udføres af retshåndhævende myndigheder, grænsekontrolmyndigheder, indvandringsmyndigheder eller asylmyndigheder. Kommissionen og AI-Udvalget tager, hvis det er relevant, hensyn til de årlige rapporter, når de udfører deres opgaver i henhold til nærværende forordning.

- 5b. Kommissionen sikrer, at oplysninger om reguleringsmæssige sandkasser for kunstig intelligens, herunder om dem, der er oprettet i henhold til denne artikel, er tilgængelige via den centrale informationsplatform, der er omhandlet i artikel 55, stk. 3, litra b).
6. De nærmere bestemmelser og betingelserne for oprettelse og anvendelse af de reguleringsmæssige sandkasser for kunstig intelligens i henhold til nærværende forordning vedtages ved gennemførelsesretsakter efter undersøgelsesproceduren i artikel 74, stk. 2.

De nærmere regler og betingelser skal i videst muligt omfang støtte de nationale kompetente myndigheders fleksibilitet til at oprette og drive deres reguleringsmæssige sandkasser for kunstig intelligens, fremme innovation og lovgivningsmæssig læring og skal navnlig tage hensyn til de deltagende SMV'ers, herunder startupvirksomheders, særlige omstændigheder og kapacitet.

Disse gennemførelsesretsakter skal indeholde fælles hovedprincipper for følgende spørgsmål:

- a) støtteberettigelse og udvælgelse med henblik på deltagelse i den reguleringsmæssige sandkasse for kunstig intelligens
 - b) proceduren for anvendelse, deltagelse, overvågning, udtræden fra og afslutning af den reguleringsmæssige sandkasse for kunstig intelligens, herunder sandkasseplanen og slutrapporten
 - c) hvilke vilkår og betingelser der gælder for deltagerne.
7. Når de nationale kompetente myndigheder overvejer at tillade prøvning under faktiske forhold under tilsyn inden for rammerne af en reguleringsmæssig sandkasse for kunstig intelligens, der er oprettet i henhold til denne artikel, aftaler de specifikt med deltagerne vilkårene og betingelserne for en sådan prøvning og navnlig de fornødne garantier med henblik på at beskytte de grundlæggende rettigheder, sundheden og sikkerheden. Hvis det er relevant, samarbejder de med andre nationale kompetente myndigheder med henblik på at sikre en ensartet praksis i hele Unionen.

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 kan personoplysninger, der er lovligt indsamlet til andre formål, behandles med henblik på udvikling og prøvning af samt undervisning i innovative AI-systemer i sandkassen på følgende kumulative betingelser:
 - a) de innovative AI-systemer skal udvikles med henblik på at beskytte væsentlige samfundsinteresser af en offentlig myndighed eller anden fysisk eller juridisk person, der henhører under offentlig ret eller privatret og på et eller flere af følgende områder:
 - i) [udgår]
 - ii) den offentlige sikkerhed og folkesundheden, herunder sygdomsforebyggelse, bekæmpelse og behandling samt forbedring af sundhedssystemerne
 - iii) beskyttelse og forbedring af miljøkvaliteten, herunder grøn omstilling, modvirkning af og tilpasning til klimaændringer
 - iv) energimæssig bæredygtighed, transport og mobilitet
 - v) effektivitet og kvalitet i den offentlige forvaltning og offentlige tjenester
 - vi) cybersikkerhed og kritiske enheders modstandsdygtighed
 - 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 rettigheder og frihedsrettigheder, jf. artikel 35 i forordning (EU) 2016/679 og artikel 39 i forordning (EU) 2018/1725, 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, der ikke er deltagere i sandkassen, medmindre en sådan videregivelse sker i overensstemmelse med forordning (EU) 2016/679 eller, hvis det er relevant, forordning 2018/725, og alle deltagere har indvilliget heri
- f) enhver behandling af personoplysninger i forbindelse med sandkassen berører ikke anvendelsen af de registreredes rettigheder i henhold til EU-retten om beskyttelse af personoplysninger, navnlig artikel 22 i forordning (EU) 2016/679 og artikel 24 i forordning (EU) 2018/1725
- g) alle personoplysninger, der skal behandles i forbindelse med sandkassen, skal beskyttes gennem passende tekniske og organisatoriske foranstaltninger og slettes, når deltagelsen i sandboksen afsluttes, eller når opbevaringsperioden for personoplysningerne udløber
- h) logfilerne over behandlingen af personoplysninger i forbindelse med sandkassen opbevares, så længe de deltager i sandkassen, medmindre andet er fastsat i EU-retten eller national ret
- 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.
Denne forpligtelse omfatter ikke følsomme operationelle oplysninger i forbindelse med aktiviteter, der udføres af retshåndhævende myndigheder, grænsekontrolmyndigheder, indvandringsmyndigheder eller asylmyndigheder.

- 1a. Med henblik på at forebygge, efterforske, opdage eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed, under de retshåndhævende myndigheders kontrol og ansvar, baseres behandlingen af personoplysninger i reguleringsmæssige sandkasser for kunstig intelligens på en bestemt medlemsstats ret eller EU-retten og på de samme kumulative betingelser som omhandlet i stk. 1.
2. Stk. 1 berører ikke EU's eller medlemsstaternes lovgivning, der fastsætter grundlaget for behandling af personoplysninger, hvilket er nødvendigt med henblik på udvikling, prøvning og uddannelse af innovative AI-systemer eller ethvert andet retsgrundlag i overensstemmelse med EU-retten om beskyttelse af personoplysninger.

Artikel 54a

Prøvning af højrisiko-AI-systemer under faktiske forhold uden for reguleringsmæssige sandkasser for kunstig intelligens

1. Prøvning af AI-systemer under faktiske forhold uden for reguleringsmæssige sandkasser for kunstig intelligens kan udføres af udbydere eller potentielle udbydere af højrisiko-AI-systemer, der er opført i bilag III, i overensstemmelse med bestemmelserne i denne artikel og den plan for prøvning under faktiske forhold, der er omhandlet i denne artikel.

De nærmere elementer i planen for prøvning under faktiske forhold præciseres i gennemførelsesretsakter, der vedtages af Kommissionen efter undersøgelsesproceduren i artikel 74, stk. 2.

Denne bestemmelse berører ikke Unionens eller medlemsstaternes lovgivning om prøvning under faktiske forhold af højrisiko-AI-systemer i forbindelse med produkter, der er omfattet af den lovgivning, der er opført i bilag II.

2. Udbydere eller potentielle udbydere kan gennemføre prøvning af de højrisiko-AI-systemer, der er omhandlet i bilag III, under faktiske forhold på et hvilket som helst tidspunkt, inden AI-systemet bringes i omsætning eller tages i brug alene eller i partnerskab med en eller flere potentielle brugere.
3. Prøvning af højrisiko-AI-systemer under faktiske forhold i henhold til denne artikel berører ikke den etiske gennemgang, der måtte være påkrævet i henhold til national ret eller EU-ret.
4. Udbydere eller potentielle udbydere må kun udføre prøvningen under faktiske forhold, hvis alle følgende betingelser er opfyldt:
 - a) udbyderen eller den potentielle udbyder har udarbejdet en plan for prøvning under faktiske forhold og forelagt den for markedsovervågningsmyndigheden i den eller de medlemsstater, hvor prøvningen skal udføres under faktiske forhold
 - b) markedsovervågningsmyndigheden i den eller de medlemsstater, hvor prøvningen under faktiske forhold skal udføres, har ikke gjort indsigelse mod prøvningen senest 30 dage efter forelæggelsen
 - c) udbyderen eller den potentielle udbyder med undtagelse af højrisiko-AI-systemer, der er omhandlet i bilag III, punkt 1, 6 og 7, inden for retshåndhævelse og forvaltning af migration, asyl og grænsekontrol og højrisiko-AI-systemer som omhandlet i bilag III, punkt 2, har registreret prøvningen under faktiske forhold i den EU-database, der er omhandlet i artikel 60, stk. 5a, med et EU-dækkende unikt identifikationsnummer og de oplysninger, der er angivet i bilag VIIa
 - d) den udbyder eller potentielle udbyder, der udfører prøvningen under faktiske forhold, er etableret i Unionen eller har udpeget en retlig repræsentant med henblik på prøvningen under faktiske forhold, som er etableret i Unionen

- e) data, der indsamles og behandles med henblik på prøvning under faktiske forhold, må ikke overføres til lande uden for Unionen, medmindre overførslen og behandlingen giver garantier svarende til dem, der er fastsat i EU-ret
- f) prøvningen under faktiske forhold varer ikke længere end nødvendigt for at nå målene og under ingen omstændigheder længere end 12 måneder
- g) personer, der tilhører sårbare grupper på grund af deres alder eller fysiske eller mentale handicap, beskyttes på passende vis
- h) [udgår]
- i) hvis en udbyder eller potentiel udbyder organiserer prøvningen under faktiske forhold i samarbejde med en eller flere potentielle brugere, er sidstnævnte blevet informeret om alle de aspekter af prøvningen, der er relevante for deres beslutning om at deltage, og har givet de relevante instrukser om, hvordan AI-systemet anvendes, jf. artikel 13 udbyderen eller den potentielle udbyder og brugeren/brugerne skal indgå en aftale, der præciserer deres roller og ansvar med henblik på at sikre overholdelse af bestemmelserne om prøvning under faktiske forhold i henhold til nærværende forordning og anden gældende EU-lovgivning og lovgivning i medlemsstaterne
- j) de personer, der er genstand for prøvningen under faktiske forhold, har givet informeret samtykke i overensstemmelse med artikel 54b, eller i tilfælde af retshåndhævelse, hvis indhentning af informeret samtykke ville forhindre, at AI-systemet prøves, og selve prøvningen og resultatet af prøvningen under faktiske forhold må ikke have en negativ indvirkning på forsøgspersonen
- k) prøvningen under faktiske forhold overvåges effektivt af udbyderen eller den potentielle udbyder og brugeren/brugerne med personer, der er tilstrækkeligt kvalificerede på det relevante område og har den nødvendige kapacitet, uddannelse og bemyndigelse til at udføre deres opgaver
- l) AI-systemets forudsigelser, anbefalinger eller beslutninger kan effektivt omgøres eller tilsidesættes.

5. Enhver forsøgsperson, der medvirker i prøvningen under faktiske forhold, eller vedkommendes retligt udpegede repræsentant, alt efter hvad der er relevant, kan, uden at det medfører ulemper og uden at skulle give nogen begrundelse, trække sig tilbage fra prøvningen på et hvilket som helst tidspunkt ved at tilbagekalde sit informerede samtykke. Tilbagekaldelsen af det informerede samtykke berører ikke de aktiviteter, der allerede er udført, og anvendelsen af data, der er indhentet på grundlag af det informerede samtykke, inden det blev trukket tilbage.
6. Enhver alvorlig hændelse, der konstateres under prøvningen under faktiske forhold, indberettes til den nationale markedsovervågningsmyndighed i overensstemmelse med artikel 62 i nærværende forordning. Udbyderen eller den potentielle udbyder skal straks træffe afbødende foranstaltninger eller, hvis dette ikke er muligt, suspendere prøvningen under faktiske forhold, indtil en sådan afhjælpning finder sted eller på anden måde bringer den til ophør. Udbyderen eller den potentielle udbyder skal indføre en procedure for øjeblikkelig tilbagekaldelse af AI-systemet efter en sådan afslutning af prøvningen under faktiske forhold.
7. Udbydere eller potentielle udbydere skal underrette den nationale markedsovervågningsmyndighed i den eller de medlemsstater, hvor prøvningen under faktiske forhold skal udføres, om suspensionen eller afslutningen af prøvningen under faktiske forhold og de endelige resultater.
8. Udbyderen og den potentielle udbyder er ansvarlige i henhold til gældende EU-lovgivning og lovgivning i medlemsstaterne om erstatningsansvar for enhver skade, der forvoldes i forbindelse med deres deltagelse i prøvningen under faktiske forhold.

Artikel 54b

Informeret samtykke til at deltage i prøvning under faktiske forhold uden for reguleringsmæssige sandkasser for kunstig intelligens

1. Med henblik på prøvning under faktiske forhold i henhold til artikel 54a skal forsøgspersonen frit give informeret samtykke, inden vedkommende deltager i sådanne forsøg, og efter at være blevet behørigt informeret med præcise, klare, relevante og forståelige oplysninger om:

- i) prøvningens art og formål under faktiske forhold og hvilke mulige ulemper, der kan være forbundet med vedkommendes deltagelse
 - ii) de betingelser, hvorunder prøvningen under faktiske forhold skal udføres, herunder den forventede varighed af forsøgspersonens deltagelse
 - iii) forsøgspersonens rettigheder og garantier for så vidt angår deltagelse, navnlig retten til at nægte at deltage i undersøgelsen af ydeevne samt retten til når som helst at udgå af prøvningen under faktiske forhold, uden at det er til skade for vedkommende og uden at skulle give en begrundelse herfor
 - iv) de nærmere bestemmelser for anmodning om omgørelse eller tilsidesættelse af AI-systemets forudsigelser, anbefalinger eller afgørelser
 - v) det unikke EU-dækkende identifikationsnummer for prøvningen under faktiske forhold i overensstemmelse med artikel 54a, stk. 4c, og kontaktoplysninger for den udbyder eller dennes retlige repræsentant, hos hvem der kan indhentes yderligere oplysninger.
2. Det informerede samtykke skal dateres og dokumenteres, og der skal gives en kopi til forsøgspersonen eller dennes retlige repræsentant.

Artikel 55

Støtteforanstaltninger for operatører, herunder SMV'er og startupvirksomheder

1. Medlemsstaterne skal træffe følgende foranstaltninger:
- a) give SMV'er, herunder startupvirksomheder, prioriteret adgang til de reguleringsmæssige sandkasser for kunstig intelligens, i det omfang de opfylder betingelserne for deltagelse og udvælgelse deri
 - b) organisere specifikke oplysnings- og uddannelsesaktiviteter om anvendelsen af nærværende forordning, der er skræddersyet til behovene hos SMV'er, herunder startupvirksomheder, og, hvis det er relevant, lokale offentlige myndigheder

- c) etablere en særlig kommunikationskanal med SMV'er, herunder startupvirksomheder og, hvis det er relevant, lokale offentlige myndigheder for at yde rådgivning og besvare forespørgsler om gennemførelsen af nærværende forordning, herunder for så vidt angår deltagelse i reguleringsmæssige sandkasser for kunstig intelligens.
- 2. Der skal tages hensyn til SMV-udbyderes og herunder startupvirksomheders særlige interesser og behov ved fastsættelsen af gebyrerne for overensstemmelsesvurdering i henhold til artikel 43, idet gebyrerne nedsættes i forhold til deres størrelse, markedsstørrelse og andre relevante indikatorer.
- 3. Kommissionen træffer følgende foranstaltninger:
 - a) efter anmodning fra AI-Udvalget at tilvejebringe standardiserede skabeloner for de områder, der er omfattet af nærværende forordning
 - b) at udvikle og vedligeholde en fælles informationsplatform, der giver alle operatører i hele Unionen letanvendelige oplysninger i forbindelse med nærværende forordning
 - c) at tilrettelægge passende kommunikationskampagner for at øge bevidstheden om de forpligtelser, der følger af nærværende forordning
 - d) at evaluere og fremme konvergensen af bedste praksis i offentlige udbudsprocedurer i forbindelse med AI-systemer.

Artikel 55a

Undtagelser for særlige operatører

1. Forpligtelserne i artikel 17 i nærværende forordning finder ikke anvendelse på mikrovirksomheder som defineret i artikel 2, stk. 3, i bilaget til Kommissionens henstilling 2003/361/EF om definitionen af mikrovirksomheder, små og mellemstore virksomheder, forudsat at disse virksomheder ikke har partnervirksomheder eller tilknyttede virksomheder som defineret i artikel 3 i samme bilag.
2. Stk. 1 skal ikke fortolkes således, at det fritager disse operatører for at opfylde andre krav og forpligtelser, der er fastsat i nærværende forordning, herunder dem, der er fastsat i artikel 9, 61 og 62.
3. De krav og forpligtelser vedrørende AI-systemer til generelle formål, der er fastsat i artikel 4b, finder ikke anvendelse på mikrovirksomheder og små og mellemstore virksomheder, forudsat at disse virksomheder ikke har partnervirksomheder eller tilknyttede virksomheder som defineret i artikel 3 i bilaget til Kommissionens henstilling 2003/361/EF om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

AFSNIT VI

FORVALTNING

KAPITEL 1

DET EUROPÆISKE UDVALG FOR KUNSTIG INTELLIGENS

Artikel 56

Oprettelse af Det Europæiske Udvalg for Kunstig Intelligens og strukturen heraf

1. Der oprettes et "Europæisk Udvalg for Kunstig Intelligens" ("udvalget").
2. Udvalget består af én repræsentant pr. medlemsstat. Den Europæiske Tilsynsførende for Databeskyttelse deltager som observatør. Kommissionen deltager også i udvalgets møder uden stemmeret.

Udvalget kan indbyde andre nationale myndigheder, organer eller eksperter og EU-myndigheder, organer eller eksperter til møderne fra sag til sag, hvis de drøftede spørgsmål er relevante for dem.

- 2a. Hver repræsentant udpeges af deres medlemsstat for en periode på tre år, der kan forlænges én gang.
- 2aa. Medlemsstaterne sikrer, at deres repræsentanter i udvalget:
 - i) har de relevante kompetencer og beføjelser i deres medlemsstat til at kunne bidrage aktivt til udførelsen af udvalgets opgaver, jf. artikel 58
 - ii) udpeges som eneste kontaktpunkt for udvalget og, hvor det er relevant, idet der tages hensyn til medlemsstaternes behov, som eneste kontaktpunkt for interessenter

iii) har beføjelse til at fremme sammenhæng og koordinering mellem de nationale kompetente myndigheder i deres medlemsstat for så vidt angår gennemførelsen af denne forordning, herunder gennem indsamling af relevante data og oplysninger med henblik på udførelse af deres opgaver i udvalget.

3. De udpegede repræsentanter for medlemsstaterne vedtager udvalgets forretningsorden med to tredjedeles flertal.

Forretningsordenen fastlægger navnlig procedurer for udvælgelsesprocessen, mandatets varighed og en beskrivelse af formandskabets opgaver, afstemningsreglerne og tilrettelæggelsen af udvalgets og dets undergruppers aktiviteter.

Udvalget nedsætter en stående undergruppe, der skal fungere som en platform, via hvilken interessenter kan rådgive udvalget om alle spørgsmål vedrørende gennemførelsen af denne forordning, herunder om udarbejdelsen af gennemførelsesretsakter og delegerede retsakter. Med henblik herpå indbydes organisationer, der repræsenterer interesserne hos udbydere og brugere af AI-systemer, herunder SMV'er og startupvirksomheder, samt civilsamfundsorganisationer, repræsentanter for berørte personer, forskere, standardiseringsorganisationer, bemyndigede organer, laboratorier og prøvnings- og forsøgsfaciliteter til at deltage i denne undergruppe. Udvalget opretter to stående undergrupper for at tilvejebringe en platform for samarbejde og udveksling mellem markedsovervågningsmyndighederne og de bemyndigende myndigheder om spørgsmål vedrørende henholdsvis markedsovervågning og bemyndigede organer.

Udvalget kan efter behov nedsætte andre stående eller midlertidige undergrupper med henblik på at behandle specifikke spørgsmål. Hvor det er relevant, kan de interessenter, der er omhandlet i foregående afsnit, indbydes til sådanne undergrupper eller til specifikke møder i disse undergrupper som observatører.

3a. Udvalget skal være organiseret og arbejde på en sådan måde, at der i dets arbejde sikres objektivitet og uvildighed.

4. Udvalgets formandskab varetages af en af repræsentanterne for medlemsstaterne. Efter anmodning fra formandskabet indkalder Kommissionen 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.

Artikel 57

[udgår]

Artikel 58

Udvalgets opgaver

Udvalget rådgiver og bistår Kommissionen og medlemsstaterne med henblik på at fremme en ensartet og effektiv anvendelse af denne forordning. Med henblik herpå kan udvalget navnlig:

- a) indsamle og udveksle teknisk og reguleringsmæssig ekspertise og bedste praksis blandt medlemsstaterne
- b) bidrage til harmoniseringen af den administrative praksis i medlemsstaterne, herunder i forbindelse med undtagelsen fra de overensstemmelsesvurderingsprocedurer, der er omhandlet i artikel 47, reguleringsmæssige sandkassers funktion og prøvning under faktiske forhold som omhandlet i artikel 53, 54 og 54a
- c) efter anmodning fra Kommissionen eller på eget initiativ fremsætte henstillinger og afgive skriftlige udtalelser om alle relevante spørgsmål vedrørende gennemførelsen af denne forordning og dens ensartede og effektive anvendelse, herunder:
 - 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
- d) rådgive Kommissionen om det potentielle behov for at ændre bilag III i overensstemmelse med artikel 4 og 7 under hensyntagen til relevant tilgængeligt bevismateriale og den seneste teknologiske udvikling
- e) rådgive Kommissionen under udarbejdelsen af delegerede retsakter eller gennemførelsesretsakter i henhold til denne forordning
- f) samarbejde, hvor det er relevant, med relevante EU-organer, -ekspertgrupper og -netværk, navnlig inden for produktsikkerhed, cybersikkerhed, konkurrence, digitale tjenester og medietjenester, finansielle tjenesteydelser, kryptovalutaer, forbrugerbeskyttelse, databeskyttelse og beskyttelse af grundlæggende rettigheder
- g) bidrage med og yde relevant rådgivning til Kommissionen i forbindelse med udarbejdelsen af den vejledning, der er omhandlet i artikel 58a, eller anmode om udarbejdelse af en sådan vejledning
- h) bistå markedsovervågningsmyndighederne i deres arbejde og i samarbejde og efter aftale med de pågældende markedsovervågningsmyndigheder fremme og støtte grænseoverskridende markedsovervågningsundersøgelser, herunder med hensyn til fremkomsten af systemiske risici, der kan stamme fra AI-systemer
- i) bidrage til vurderingen af uddannelsesbehov for personale i de medlemsstater, der er involveret i gennemførelsen af denne forordning
- j) rådgive Kommissionen i forbindelse med internationale spørgsmål om kunstig intelligens.

KAPITEL 1A

RETNINGSLINJER FRA KOMMISSIONEN

Artikel 58a

Retningslinjer fra Kommissionen om gennemførelsen af denne forordning

1. Efter anmodning fra medlemsstaterne eller udvalget eller på eget initiativ udsteder Kommissionen retningslinjer for den praktiske gennemførelse af denne forordning, og navnlig om
 - i) anvendelsen af de krav, der er omhandlet i artikel 8-15
 - ii) de forbudte praksisser, der er omhandlet i artikel 5
 - iii) den praktiske gennemførelse af bestemmelserne om væsentlig ændring
 - iv) den praktiske gennemførelse af de ensartede betingelser, der er omhandlet i artikel 6, stk. 3, herunder eksempler i forbindelse med højrisiko-AI-systemer som omhandlet i bilag III
 - v) den praktiske gennemførelse af gennemsigtighedsforpligtelserne i artikel 52
 - vi) forholdet mellem denne forordning og anden relevant EU-lovgivning, herunder for så vidt angår konsekvens i håndhævelsen heraf.

Når Kommissionen udsteder sådanne retningslinjer, skal den være særlig opmærksom på behovene hos SMV'er, herunder startupvirksomheder, lokale offentlige myndigheder og i sektorer, der med størst sandsynlighed vil blive berørt af denne forordning.

KAPITEL 2

NATIONALE KOMPETENTE MYNDIGHEDER

Artikel 59

Udpegelse af nationale kompetente myndigheder

1. [udgår]
2. Hver medlemsstat opretter eller udpeger mindst én bemyndigende myndighed og mindst én markedsovervågningsmyndighed som nationale kompetente myndigheder med henblik på denne forordning. Disse nationale kompetente myndigheder skal være organiseret på en sådan måde, at principperne om objektivitet og upartiskhed sikres i deres aktiviteter og opgaver. Forudsat at disse principper overholdes, kan sådanne aktiviteter og opgaver udføres af en eller flere udpegede myndigheder i overensstemmelse med medlemsstatens organisatoriske behov.
3. Medlemsstaterne underretter Kommissionen om deres udpegelse(r).
4. Medlemsstaterne sikrer, at de nationale kompetente myndigheder modtager tilstrækkelige finansielle ressourcer, tilstrækkeligt teknisk udstyr og tilstrækkelige velkvalificerede menneskelige ressourcer til at udføre deres opgaver effektivt i henhold til denne forordning.
5. Senest *[et år efter denne forordnings ikrafttræden]* og derefter seks måneder før den frist, der er omhandlet i artikel 84, stk. 2, underretter medlemsstaterne Kommissionen om status for de nationale kompetente myndigheders finansielle ressourcer, tekniske udstyr 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 rådgivning om gennemførelsen af denne forordning, herunder skræddersyet til SMV-udbydere, herunder startupvirksomheder. 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 HØJRIKIO-AI-SYSTEMER OPFØRT I BILAG III

Artikel 60

EU-database for højrisiko-AI-systemer opført i bilag III

1. Kommissionen opretter og vedligeholder i samarbejde med medlemsstaterne en EU-database med de i stk. 2 omhandlede oplysninger vedrørende relevante operatører og højrisiko-AI-systemer, jf. bilag III, som registreres i overensstemmelse med artikel 51 og 54a. Ved fastsættelsen af funktionsspecifikationerne for en sådan database hører Kommissionen AI-Udvalget.

2. De data, der er anført i bilag VIII, del I, indlæses i EU-databasen af udbyderne, de bemyndigede repræsentanter og relevante brugere, alt efter hvad der er relevant, når de registreres. De data, der er anført i bilag VIII, del II, punkt 1-11, indlæses i EU-databasen af udbyderne eller, hvor det er relevant, den bemyndigede repræsentant i overensstemmelse med artikel 51. De data, der er omhandlet i bilag VIII, del II, punkt 12, genereres automatisk af databasen på grundlag af oplysninger fra relevante brugere i henhold til artikel 51, stk. 2. De data, der er anført i bilag VIIIA, indlæses i databasen af potentielle udbydere eller udbydere i overensstemmelse med artikel 54a.
3. [udgår]
4. EU-databasen må ikke indeholde personoplysninger, bortset fra de oplysninger, der er anført i bilag VIII, og berører ikke artikel 70.
5. Kommissionen er dataansvarlig for EU-databasen. Den stiller tilstrækkelig teknisk og administrativ støtte til rådighed for udbydere, potentielle udbydere og brugere.
- 5a. Oplysningerne i EU-databasen, som registreres i overensstemmelse med artikel 51, skal være offentligt tilgængelige. De oplysninger, der registreres i henhold til artikel 54a, må kun være tilgængelige for markedsovervågningsmyndighederne og Kommissionen, medmindre den potentielle udbyder eller udbyderen har givet sit samtykke til, at disse oplysninger også gøres tilgængelige for offentligheden.

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 risiciene ved højrisiko-AI-systemet.
2. For at give udbyderen mulighed for at evaluere AI-systemernes overholdelse af de i afsnit III, kapitel 2, fastsatte krav i hele deres livscyklus indsamler, dokumenterer og analyserer systemet til overvågning efter omsætningen relevante data, som brugerne kan afgive, eller som kan indsamles via andre kilder, om højrisiko-AI-systemers ydeevne. Denne forpligtelse omfatter ikke følsomme operationelle data om brugere af AI-systemer, som er retshåndhævende myndigheder.
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 i bilag II, afsnit A, opførte retsakter, hvor der allerede er etableret et system til og en plan for overvågning efter omsætningen i henhold til nævnte lovgivning, anses dokumentationen for overvågning efter omsætningen som udarbejdet i henhold til nævnte lovgivning for at være tilstrækkelig, forudsat at den i stk. 3 omhandlede model er anvendt.

Første afsnit finder også anvendelse på de i bilag III, punkt 5, omhandlede højrisiko-AI-systemer, der bringes i omsætning eller tages i brug af finansielle institutioner, der er underlagt krav vedrørende deres interne forvaltning, ordninger eller processer i henhold til EU-lovgivningen om finansielle tjenesteydelser.

KAPITEL 2

UDVEKSLING AF OPLYSNINGER OM ALVORLIGE HÆNDELSER

Artikel 62

Indberetning af alvorlige hændelser

1. Udbydere af højrisiko-AI-systemer, der bringes i omsætning på EU-markedet, indberetter enhver alvorlig hændelse til markedsovervågningsmyndighederne i de medlemsstater, hvor hændelsen fandt sted.

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

2. Når den relevante markedsovervågningsmyndighed modtager en indberetning vedrørende en alvorlig hændelse som omhandlet i artikel 3, nr. 44, litra c), underretter den 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, omhandlede højrisiko-AI-systemer, der bringes i omsætning eller tages i brug af udbydere, som er finansielle institutioner, der er underlagt krav vedrørende deres interne forvaltning, ordninger eller processer i henhold til EU-lovgivningen om finansielle tjenesteydelser, begrænses indberetningen af alvorlige hændelser til dem, der er omhandlet i artikel 3, nr. 44, litra c).
4. For højrisiko-AI-systemer, som er 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 til dem, der er omhandlet i artikel 3, nr. 44, litra c), og foretages til den nationale kompetente myndighed, som er valgt til dette formål af den medlemsstat, hvor hændelsen fandt sted.

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 artikel 2 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. Som led i deres rapporteringsforpligtelser i henhold til artikel 34, stk. 4, i forordning (EU) 2019/1020 aflægges markedsovervågningsmyndighederne rapport til Kommissionen om resultaterne af relevante markedsovervågningsaktiviteter i henhold til nærværende forordning.
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, eller under begrundede omstændigheder, og forudsat at der sikres koordinering, en anden relevant myndighed som fastlagt af medlemsstaten.

De procedurer, der er omhandlet i denne forordnings artikel 65, 66, 67 og 68, finder ikke anvendelse på AI-systemer i forbindelse med produkter, som de retsakter, der er opført i bilag II, afsnit A, finder anvendelse på, når sådanne retsakter allerede indeholder bestemmelser om procedurer med samme formål. I sådanne tilfælde finder disse sektorprocedurer anvendelse i stedet.

4. For så vidt angår højrisiko-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 nationale myndighed, der i henhold til nævnte lovgivning er ansvarlig for det finansielle tilsyn med disse institutioner, såfremt omsætningen, ibrugtagningen eller anvendelsen af AI-systemet er i direkte forbindelse med leveringen af disse finansielle tjenesteydelser.

Uanset det foregående afsnit kan medlemsstaten under begrundede omstændigheder, og forudsat at der sikres koordinering, udpege en anden relevant myndighed som markedsovervågningsmyndighed med henblik på denne forordning.

Nationale markedsovervågningsmyndigheder, som fører tilsyn med kreditinstitutter, der er reguleret i henhold til direktiv 2013/36/EU, og som deltager i den fælles tilsynsmekanisme (FTM), der er oprettet ved Rådets forordning (EF) nr. 1204/2013, bør straks indberette alle oplysninger, som er identificeret i forbindelse med deres markedsovervågningsaktiviteter, og som kan være af potentiel interesse for Den Europæiske Centralbanks tilsynsopgaver som fastsat i nævnte forordning, til Den Europæiske Centralbank.

5. For så vidt angår de højrisiko-AI-systemer, der er anført i punkt 1, litra a), i det omfang systemerne anvendes til retshåndhævelsesformål, jf. punkt 6, 7 og 8 i bilag III, udpeger medlemsstaterne med henblik på denne forordning som markedsovervågningsmyndigheder enten de nationale myndigheder, der fører tilsyn med de retshåndhævende myndigheders, grænsekontrol-, indvandrings- eller asylmyndighedernes eller de retlige myndigheders aktiviteter, eller de kompetente datatilsynsmyndigheder i henhold til direktiv (EU) 2016/680 eller forordning 2016/679. Markedsovervågningsaktiviteter må på ingen måde påvirke de retlige myndigheders uafhængighed eller på anden måde gribe ind i deres aktiviteter, når de handler i deres egenskab af domstol.
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.
8. Uden at det berører de beføjelser, der er fastsat i forordning (EU) 2019/1020, og hvor det er relevant og begrænset til, hvad der er nødvendigt for, at markedsovervågningsmyndighederne kan udføre deres opgaver, gives de af udbyderen fuld adgang til den dokumentation samt til de trænings-, validerings- og prøvningsdatasæt, der anvendes til udvikling af højrisiko-AI-systemet, herunder, hvor det er relevant og med forbehold af sikkerhedsforanstaltninger, via programmeringsgrænseflader for applikationer ("API'er") eller andre relevante tekniske midler og værktøjer, der muliggør fjernadgang.
9. Markedsovervågningsmyndighederne gives efter begrundet anmodning adgang til kildekoden for højrisiko-AI-systemet, og kun når følgende kumulative betingelser er opfyldt:

- a) Adgang til kildekode er nødvendig for at vurdere, om et højrisiko-AI-system er i overensstemmelse med kravene i afsnit III, kapitel 2, og
- b) prøvnings-/revisionsprocedurer og verificeringer på grundlag af data og dokumentation fra udbyderen er udtømt eller har vist sig at være utilstrækkelige.

- 10. Alle oplysninger og al dokumentation, som markedsovervågningsmyndighederne modtager, behandles i overensstemmelse med tavshedspligten, jf. artikel 70.
- 11. Klager til den relevante markedsovervågningsmyndighed kan indgives af enhver fysisk eller juridisk person, der har grund til at mene, at der er sket en overtrædelse af bestemmelserne i denne forordning.

I overensstemmelse med artikel 11, stk. 3, litra e), og stk. 7, litra a), i forordning (EU) 2019/1020 tages klager i betragtning med henblik på at udføre markedsovervågningsaktiviteterne og behandles i overensstemmelse med de særlige procedurer, som markedsovervågningsmyndighederne har fastlagt dertil.

Artikel 63a

Markedsovervågningsmyndighedernes tilsyn med prøvning under faktiske forhold

- 1. Markedsovervågningsmyndighederne skal have kompetence og beføjelser til at sikre, at prøvning under faktiske forhold er i overensstemmelse med denne forordning.
- 2. Hvis der udføres prøvning under faktiske forhold for AI-systemer, som der føres tilsyn med i den reguleringsmæssige sandkasse for kunstig intelligens i henhold til artikel 54, kontrollerer markedsovervågningsmyndighederne overholdelsen af bestemmelserne i artikel 54a som led i deres tilsynsrolle for den reguleringsmæssige sandkasse for kunstig intelligens. Disse myndigheder kan, hvor det er relevant, tillade, at prøvningen under faktiske forhold udføres af udbyderen eller den potentielle udbyder som en undtagelse fra betingelserne i artikel 54a, stk. 4, litra f) og g).

3. Hvis en markedsovervågningsmyndighed er blevet underrettet af den potentielle udbyder, udbyderen eller enhver tredjepart om en alvorlig hændelse eller har andre grunde til at mene, at betingelserne i artikel 54a og 54b ikke er opfyldt, kan den træffe en af følgende afgørelser på sit område, alt efter hvad der er relevant:
 - a) suspendere eller afslutte prøvningen under faktiske forhold
 - b) kræve, at udbyderen eller den potentielle udbyder og brugeren eller brugerne ændrer et hvilket som helst aspekt af prøvningen under faktiske forhold.
4. Hvis en markedsovervågningsmyndighed har truffet en afgørelse som omhandlet i denne artikels stk. 3 eller har gjort indsigelse som omhandlet i artikel 54a, stk. 4, litra b), skal afgørelsen eller indsigelsen indeholde en begrundelse herfor samt de nærmere bestemmelser og betingelser for, at udbyderen eller den potentielle udbyder kan anfægte afgørelsen eller indsigelsen.
5. Hvis en markedsovervågningsmyndighed har truffet en afgørelse som omhandlet i denne artikels stk. 3, meddeler den, hvor det er relevant, begrundelsen herfor til markedsovervågningsmyndighederne i de andre medlemsstater, hvor AI-systemet er blevet prøvet i overensstemmelse med planen for prøvning.

Artikel 64

Beføjelser tillagt myndigheder, der beskytter de grundlæggende rettigheder

1. [udgår]
2. [udgår]

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, herunder retten til retten til beskyttelse mod forskelsbehandling, 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 tre måneder efter denne forordnings ikrafttræden identificerer hver medlemsstat de offentlige myndigheder eller organer, der er omhandlet i stk. 3, og offentliggør listen. 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 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 identificeres risici for 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, anmoder den uden unødigt forsinkelse 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 tidsfrist, som den fastsætter.

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, underretter den uden unødigt forsinkelse 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 underretter uden unødigt forsinkelse Kommissionen og de øvrige medlemsstater om sådanne foranstaltninger.
6. Den i stk. 5 omhandlede underretning skal indeholde alle tilgængelige oplysninger, særlig de nødvendige oplysninger 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) manglende overholdelse af forbuddet mod de i artikel 5 anførte former for praksis med hensyn til kunstig intelligens
 - a) et højrisiko-AI-systems 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.
 - c) manglende overholdelse af bestemmelserne i artikel 52
 - d) AI-systemer til generelle formål, som ikke overholder de krav og forpligtelser, der er omhandlet i artikel 4a.

7. Markedsovervågningsmyndighederne i de andre medlemsstater end markedsovervågningsmyndigheden i den medlemsstat, der har indledt proceduren, underretter uden unødigt forsinkelse 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 den i stk. 5 omhandlede underretning 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. Den periode, der er omhandlet i dette stykkes første punktum, nedsættes til 30 dage i tilfælde af manglende overholdelse af forbuddet mod de i artikel 5 anførte former for praksis med hensyn til kunstig intelligens.
9. Markedsovervågningsmyndighederne i samtlige medlemsstater sikrer derefter, at der uden unødigt forsinkelse træffes de fornødne restriktive foranstaltninger med hensyn til det pågældende AI-system, 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 eller 30 dage i tilfælde af manglende overholdelse af forbuddet mod de i artikel 5 anførte former for praksis med hensyn til kunstig intelligens 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 uden unødigt forsinkelse spørgsmålet med den relevante medlemsstats markedsovervågningsmyndighed og den eller de relevante operatører og evaluerer den nationale foranstaltning. På grundlag af resultaterne af denne evaluering træffer Kommissionen senest ni måneder efter den i artikel 65, stk. 5, omhandlede underretning afgørelse om, hvorvidt den nationale foranstaltning er berettiget eller ej, eller 60 dage i tilfælde af manglende overholdelse af forbuddet mod de i artikel 5 anførte former for praksis med hensyn til kunstig intelligens. Den meddeler den pågældende medlemsstat en sådan afgørelse. Kommissionen underretter også alle andre medlemsstater om en sådan afgørelse.
2. Hvis Kommissionen anser den foranstaltning, der er truffet af den relevante medlemsstats markedsovervågningsmyndighed, for at være berettiget, sikrer markedsovervågningsmyndighederne i samtlige medlemsstater, at der træffes de fornødne restriktive foranstaltninger med hensyn til det pågældende AI-system, f.eks. tilbagetrækning af AI-systemet fra deres marked uden unødigt forsinkelse, og underretter Kommissionen herom. Hvis Kommissionen anser den nationale foranstaltning for ikke at være berettiget, trækker den pågældende medlemsstats markedsovervågningsmyndighed foranstaltningen tilbage og underretter Kommissionen herom.
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

Højrisiko-AI-systemer eller AI-systemer til generelle formål, 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 højrisiko-AI-system eller AI-system til generelle formål, selv om det opfylder kravene i denne forordning, udgør en risiko for menneskers sundhed eller sikkerhed eller for de grundlæggende rettigheder, skal den pålægge den relevante 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 sådan risiko, eller for at trække AI-systemet tilbage fra markedet eller kalde det tilbage uden unødigt forsinkelse, inden for en tidsfrist, som den fastsætter.
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 uden unødigt forsinkelse spørgsmålet med de pågældende medlemsstater og den relevante 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 de pågældende medlemsstater og underretter alle andre medlemsstater.

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, inden for tidsfrist, som den fastsætter:
 - 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.

Artikel 68a

EU-prøvningsfaciliteter på området kunstig intelligens

1. Kommissionen udpeger en eller flere EU-prøvningsfaciliteter i henhold til artikel 21 i forordning (EU) 2019/1020 på området kunstig intelligens.

2. Uden at det berører EU-prøvningsfaciliteternes aktiviteter som omhandlet i artikel 21, stk. 6, i forordning (EU) 2019/1020, skal de i stk. 1 omhandlede EU-prøvningsfaciliteter også yde uafhængig teknisk eller videnskabelig rådgivning efter anmodning fra udvalget eller markedsovervågningsmyndighederne.

Artikel 68b

Central pulje af uafhængige eksperter

1. Efter anmodning fra AI-Udvalget fastsætter Kommissionen ved hjælp af en gennemførelsesretsakt bestemmelser om oprettelse, vedligeholdelse og finansiering af en central pulje af uafhængige eksperter til støtte for håndhævelsesaktiviteterne i henhold til denne forordning.
2. Eksperterne udvælges af Kommissionen og medtages i den centrale pulje på grundlag af ajourført videnskabelig eller teknisk ekspertise inden for kunstig intelligens under behørig hensyntagen til de tekniske områder, der er omfattet af kravene og forpligtelserne i denne forordning, og markedsovervågningsmyndighedernes aktiviteter i henhold til artikel 11 i forordning (EU) 2019/1020. Kommissionen fastsætter antallet af medlemmer i puljen i overensstemmelse med, hvad der er behov for.
3. Eksperterne kan have følgende opgaver:
 - a) yde rådgivning til markedsovervågningsmyndighederne og støtte deres arbejde efter disses anmodning
 - b) støtte grænseoverskridende markedsovervågningsundersøgelser som omhandlet i artikel 58, litra h), uden at dette berører markedsovervågningsmyndighedernes beføjelser
 - c) rådgive og bistå Kommissionen i udførelsen af dens opgaver inden for rammerne af beskyttelsesklausulen i henhold til artikel 66.

4. Ekspertene udfører deres opgaver uvildigt og objektivt og sikrer fortroligheden af de oplysninger og data, der er indhentet under udførelsen af deres opgaver og aktiviteter. Hver ekspert udfærdiger en interesseerklæring, der gøres offentligt tilgængelig. Kommissionen etablerer systemer og procedurer til aktivt at håndtere og forebygge potentielle interessekonflikter.
5. Medlemsstaterne kan pålægges at betale gebyrer for eksperternes rådgivning og støtte. Gebyrernes struktur og størrelse samt størrelsen og strukturen af de omkostninger, der kan kræves erstattet, vedtages af Kommissionen ved hjælp af den gennemførelsesretsakt, der er omhandlet i stk. 1, under hensyntagen til målene om en passende gennemførelse af denne forordning, omkostningseffektivitet og nødvendigheden af at sikre, at alle medlemsstater har effektiv adgang til eksperter.
6. Kommissionen fremmer rettidig adgang til eksperterne for medlemsstaterne efter behov og sikrer, at kombinationen af støtteaktiviteter, som udføres af EU-prøvningsfaciliteter i henhold til artikel 68a, og eksperter i henhold til denne artikel tilrettelægges effektivt og giver den bedst mulige merværdi.

AFSNIT IX

ADFÆRDSKODEKSER

Artikel 69

Adfærdskodekser for frivillig anvendelse af specifikke krav

1. Kommissionen og medlemsstaterne letter udarbejdelsen af adfærdskodekser, der har til formål at tilskynde til frivillig anvendelse af et eller flere af de i denne forordnings afsnit III, kapitel 2, fastsatte krav på AI-systemer, der ikke er højrisiko-AI-systemer, i videst muligt omfang under hensyntagen til de tilgængelige tekniske løsninger, der gør det muligt at anvende disse krav.
2. Kommissionen og medlemsstaterne letter udarbejdelsen af adfærdskodekser, der har til formål at tilskynde til frivillig anvendelse på alle AI-systemer af specifikke krav vedrørende f.eks. miljømæssig bæredygtighed, herunder med hensyn til energieffektiv programmering, 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. Kommissionen og medlemsstaterne letter også, hvor det er relevant, udarbejdelsen af adfærdskodekser, der finder anvendelse på frivillig basis med hensyn til brugernes forpligtelser i forbindelse med AI-systemer.
3. Adfærdskodekser, der finder anvendelse på frivillig basis, 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, eller, hvor det er relevant, af brugere med hensyn til deres forpligtelser. Adfærdskodekser kan omfatte et eller flere AI-systemer under hensyntagen til ligheden mellem de relevante systemers tilsigtede formål.
4. Når Kommissionen og medlemsstaterne tilskynder til og letter udarbejdelsen af de i denne artikel omhandlede adfærdskodekser, tager de hensyn til SMV-udbyderes, herunder startupvirksomheders, særlige interesser og behov.

AFSNIT X

TAVSHEDSPLIGT OG SANKTIONER

Artikel 70

Tavshedspligt

1. De nationale kompetente myndigheder, bemyndigede organer, Kommissionen, udvalget og enhver anden fysisk eller juridisk person, der er involveret i anvendelsen af denne forordning, skal i overensstemmelse med EU-retten eller national ret indføre passende tekniske og organisatoriske foranstaltninger for at sikre 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
 - c) offentlige og nationale sikkerhedsinteresser
 - d) strafferetlige eller administrative procedurers integritet
 - e) integriteten af informationer, der er klassificeret i overensstemmelse med EU-retten eller national ret.

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, grænsekontrolmyndigheder, indvandringsmyndigheder eller asylmyndigheder, hvis en sådan videregivelse ville bringe offentlige og nationale sikkerhedsinteresser i fare. Denne forpligtelse til at udveksle oplysninger omfatter ikke følsomme operationelle oplysninger i forbindelse med aktiviteter, der udføres af retshåndhævende myndigheder, grænsekontrolmyndigheder, indvandringsmyndigheder eller asylmyndigheder.

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 deres relevante myndigheders eller de bemyndigede organers rettigheder og forpligtelser med hensyn til udveksling af oplysninger og udsendelse af advarsler, herunder i forbindelse med grænseoverskridende samarbejde, eller de berørte parter forpligtelse til at afgive oplysninger inden for rammerne af medlemsstaternes straffelovgivning.

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 SMV-udbydere, herunder startupvirksomheders, størrelse og interesser og deres økonomiske levedygtighed. Der skal også tages hensyn til, om anvendelsen af AI-systemet sker i forbindelse med en personlig ikkeerhvervsmæssig aktivitet.
2. Medlemsstaterne underretter straks Kommissionen om disse regler og foranstaltninger og om senere ændringer, der berører dem.
3. Manglende overholdelse af ethvert forbud mod de i artikel 5 anførte former for praksis med hensyn til kunstig intelligens, skal straffes med administrative bøder på op til 30 000 000 EUR eller, hvis lovovertræderen er en virksomhed, op til 6 % af dens samlede globale årlige omsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst. For SMV'er, herunder startupvirksomheder, skal disse bøder udgøre op til 3 % af deres globale årlige omsætning i det foregående regnskabsår.
4. Overtrædelser af følgende bestemmelser vedrørende operatører eller bemyndigede organer 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 årsomsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst:
 - a) forpligtelser for udbydere i henhold til artikel 4b og 4c
 - a) forpligtelser for udbydere i henhold til artikel 16
 - b) forpligtelser for visse andre personer i henhold til artikel 23a

- c) forpligtelser for bemyndigede repræsentanter i henhold til artikel 25
- d) forpligtelser for importører i henhold til artikel 26
- e) forpligtelser for distributører i henhold til artikel 27
- f) forpligtelser for brugere i henhold til artikel 29, stk. 1-6a
- g) krav til og forpligtelser for bemyndigede organer i henhold til artikel 33, artikel 34, stk. 1, 3 og 4, og artikel 34a
- h) gennemsigtighedsforpligtelser for udbydere og brugere i henhold til artikel 52.

For SMV'er, herunder startupvirksomheder, skal disse bøder udgøre op til 2 % af deres globale årlige omsætning i det foregående regnskabsår.

- 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. For SMV'er, herunder startupvirksomheder, skal disse bøder udgøre op til 1 % af deres globale årlige omsætning i det foregående regnskabsår.
- 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
 - aa) hvorvidt overtrædelsen blev begået forsætligt eller uagtsomt
 - ab) enhver foranstaltning, der træffes af operatøren med henblik på at afhjælpe overtrædelsen og afbøde de mulige negative virkninger af overtrædelsen

- b) hvorvidt andre markedsovervågningsmyndigheder i andre medlemsstater allerede har pålagt den samme operatør administrative bøder for samme overtrædelse
 - ba) hvorvidt andre myndigheder allerede har pålagt den samme operatør administrative bøder for overtrædelser af anden EU-ret eller national ret, når sådanne overtrædelser skyldes den samme aktivitet eller undladelse, der udgør en relevant overtrædelse af denne retsakt
 - c) størrelsen på den operatør, der har begået overtrædelsen, og dens årsomsætning og markedsandel
 - d) om der er andre skærpende eller formildende faktorer ved sagens omstændigheder, såsom opnåede økonomiske fordele eller undgåede tab som direkte eller indirekte følge af overtrædelsen.
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.
9. Markedsovervågningsmyndighedens udøvelse af beføjelser i henhold til denne artikel skal være underlagt fornødne proceduremæssige garantier i overensstemmelse med EU-retten og medlemsstaternes nationale ret, bl.a. effektive retsmidler og retfærdig procedure.

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. Manglende overholdelse af ethvert forbud mod de i artikel 5 anførte former for praksis med hensyn til kunstig intelligens, skal straffes med administrative bøder på op til 500 000 EUR.
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 7, stk. 1 og 3, artikel 11, stk. 3, artikel 43, stk. 5 og 6, og artikel 48, stk. 5, omhandlede delegation af beføjelser tillægges Kommissionen for en periode på fem år fra [datoen for denne forordnings ikrafttræden].

Kommissionen udarbejder en rapport vedrørende delegationen af beføjelser senest ni måneder inden udløbet af femårsperioden. Delegationen af beføjelser forlænges stiltiende for perioder af samme varighed, medmindre Europa-Parlamentet eller Rådet modsætter sig en sådan forlængelse senest tre måneder inden udløbet af hver periode.

3. Den i artikel 7, stk. 1 og 3, 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 7, stk. 1 og 3, 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. [udgår]
- 1b. Kommissionen vurderer behovet for at ændre listen i bilag III hver 24. måned efter denne forordnings ikrafttræden og indtil slutningen på perioden med delegation af beføjelser. Resultaterne af denne vurdering forelægges Europa-Parlamentet og Rådet.

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 ressourcer, tekniske udstyr 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, hvor det er relevant, evaluerer Kommissionen virkningen og effektiviteten af frivillige adfærdskodekser med henblik på at fremme anvendelsen af kravene i afsnit III, kapitel 2, på andre AI-systemer end højrisiko-AI-systemer, og eventuelt andre yderligere krav til AI-systemer, herunder vedrørende miljømæssig bæredygtighed.
5. Med henblik på stk. 1a-4 indgiver udvalget, medlemsstaterne og de nationale kompetente myndigheder oplysninger til Kommissionen på dennes anmodning.
6. Når Kommissionen foretager evaluering og revision, jf. stk. 1a-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 [36 måneder efter forordningens ikrafttræden].
3. Uanset stk. 2:
 - a) anvendes afsnit III, kapitel 4, og afsnit VI fra den [12 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

BILAG I
[udgår]

BILAG II

LISTE OVER EU-HARMONISERINGSLOVGIVNING

Del A – Liste over EU-harmoniseringslovgivning under den nye lovgivningsmæssige ramme

1. Europa-Parlamentets og Rådets direktiv 2006/42/EF af 17. maj 2006 om maskiner og om ændring af direktiv 95/16/EF (EUT L 157 af 9.6.2006, s. 24) [som ophævet ved maskinforordningen]
2. Europa-Parlamentets og Rådets direktiv 2009/48/EF af 18. juni 2009 om sikkerhedskrav til legetøj (EUT L 170 af 30.6.2009, s. 1)
3. Europa-Parlamentets og Rådets direktiv 2013/53/EU af 20. november 2013 om fritidsfartøjer og personlige fartøjer og om ophævelse af direktiv 94/25/EF (EUT L 354 af 28.12.2013, s. 90)
4. Europa-Parlamentets og Rådets direktiv 2014/33/EU af 26. februar 2014 om harmonisering af medlemsstaternes love om elevatorer og sikkerhedskomponenter til elevatorer (EUT L 96 af 29.3.2014, s. 251)
5. Europa-Parlamentets og Rådets direktiv 2014/34/EU af 26. februar 2014 om harmonisering af medlemsstaternes love om materiel og sikringssystemer til anvendelse i en potentielt eksplosiv atmosfære (EUT L 96 af 29.3.2014, s. 309)
6. Europa-Parlamentets og Rådets direktiv 2014/53/EU af 16. april 2014 om harmonisering af medlemsstaternes love om tilgængeliggørelse af radioudstyr på markedet og om ophævelse af direktiv 1999/5/EF (EUT L 153 af 22.5.2014, s. 62)
7. Europa-Parlamentets og Rådets direktiv 2014/68/EU af 15. maj 2014 om harmonisering af medlemsstaternes lovgivning om tilgængeliggørelse på markedet af trykbærende udstyr (EUT L 189 af 27.6.2014, s. 164)

8. Europa-Parlamentets og Rådets forordning (EU) 2016/424 af 9. marts 2016 om tovbaneanlæg og om ophævelse af direktiv 2000/9/EF (EUT L 81 af 31.3.2016, s. 1)
9. Europa-Parlamentets og Rådets forordning (EU) 2016/425 af 9. marts 2016 om personlige værnemidler og om ophævelse af Rådets direktiv 89/686/EØF (EUT L 81 af 31.3.2016, s. 51)
10. Europa-Parlamentets og Rådets forordning (EU) 2016/426 af 9. marts 2016 om apparater, der forbrænder gasformigt brændstof, og om ophævelse af direktiv 2009/142/EF (EUT L 81 af 31.3.2016, s. 99)
11. 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)
12. 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).

Del B. Liste over anden EU-harmoniseringslovgivning

1. 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)
2. 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)
3. 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)
4. Europa-Parlamentets og Rådets direktiv 2014/90/EU af 23. juli 2014 om skibsstyr og om ophævelse af Rådets direktiv 96/98/EF (EUT L 257 af 28.8.2014, s. 146)
5. 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)
6. 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)

7. 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 forordning (EF) nr. 78/2009, forordning (EF) nr. 79/2009 og Europa-Parlamentets og Rådets forordning (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)
8. 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 Europa-Parlamentets og Rådets forordning (EF) nr. 2111/2005, (EF) nr. 1008/2008, (EU) nr. 996/2010 og (EU) nr. 376/2014 og direktiv 2014/30/EU og 2014/53/EU og om ophævelse af Europa-Parlamentets og Rådets forordning (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), for så vidt angår konstruktion, fremstilling og bringe i omsætning af luftfartøjer, som er omhandlet i nævnte forordnings artikel 2, stk. 1, litra a) og b), når det drejer sig om ubemandede luftfartøjer og tilhørende motorer, propeller, dele og udstyr til fjernkontrol af disse luftfartøjer.

BILAG III
HØJRISIKO-AI-SYSTEMER, jf. artikel 6, stk. 3

På hvert af de områder, der er opført under punkt 1-8, anses de AI-systemer, der specifikt er nævnt under hvert litra, for at være højrisiko-AI-systemer i henhold til artikel 6, stk. 3:

1. Biometri:
 - a) systemer til biometrisk fjernidentifikation.
2. Kritisk infrastruktur:
 - a) AI-systemer, der er beregnet til anvendelse som sikkerhedskomponenter i forvaltningen og driften af kritisk digital infrastruktur, vejtrafik og forsyning af vand, gas, varme og elektricitet.
3. Uddannelse og erhvervsuddannelse:
 - a) AI-systemer, der er beregnet til at fastslå, om fysiske personer skal optages på eller have adgang til uddannelsesinstitutioner eller -programmer på alle niveauer, eller hvordan de skal fordeles
 - b) AI-systemer, der er beregnet til at evaluere læringsresultater, herunder når disse resultater anvendes til at styre fysiske personers læringsproces på uddannelsesinstitutioner eller -programmer på alle niveauer.
4. Beskæftigelse, forvaltning af arbejdstagere og adgang til selvstændig virksomhed:
 - a) AI-systemer, der er beregnet til rekruttering eller udvælgelse af fysiske personer, navnlig til at indrykke målrettede jobannoncer, analysere og filtrere jobansøgninger og evaluere kandidater

- b) AI-systemer, der er beregnet til at træffe afgørelser om forfremmelse og afskedigelse i arbejdsrelaterede kontraktforhold, til at fordele opgaver på grundlag af individuel adfærd eller personlighedstræk eller personlige egenskaber og til at overvåge og evaluere personers præstationer og adfærd i sådanne forhold.

5. Adgang til og benyttelse af væsentlige private tjenester og væsentlige offentlige tjenester og fordele:

- a) AI-systemer, der er beregnet til at blive anvendt af offentlige myndigheder eller på vegne af offentlige myndigheder til at vurdere fysiske personers berettigelse til væsentlige offentlige sociale ydelser og tjenester samt til at tildele, reducere, annullere eller tilbagekalde sådanne ydelser og tjenester
- b) AI-systemer, der er beregnet til at foretage kreditvurderinger af fysiske personer eller fastslå deres kreditværdighed, med undtagelse af AI-systemer, der tages i brug af udbydere, som er mikrovirksomheder og små virksomheder som defineret i bilaget til Kommissionens henstilling 2003/361/EF, til egen brug
- c) AI-systemer, der er beregnet til at sende beredskabstjenester i nødsituationer eller til at tildele prioriteter i forbindelse hermed, herunder brandslukning og lægehjælp
- d) AI-systemer, der er beregnet til at foretage risikovurdering og prisfastsættelse for så vidt angår fysiske personer i forbindelse med livs- og sygeforsikring, med undtagelse af AI-systemer, der tages i brug af udbydere, som er mikrovirksomheder og små virksomheder som defineret i bilaget til Kommissionens henstilling 2003/361/EF, til egen brug.

6. Retshåndhævelse:

- a) AI-systemer, der er beregnet til at blive anvendt af retshåndhævende myndigheder eller på deres vegne til at vurdere risikoen for, at en fysisk person begår eller genbegår lovovertrædelser eller bliver potentielt offer for strafbare handlinger

- b) AI-systemer, der er beregnet til at blive anvendt af retshåndhævende myndigheder eller på deres vegne som polygrafer og lignende værktøjer eller til at påvise en fysisk persons følelsesmæssige tilstand
- c) [udgår]
- d) AI-systemer, der er beregnet til at blive anvendt af retshåndhævende myndigheder eller på deres vegne til at vurdere pålideligheden af bevismateriale i forbindelse med efterforskning eller retsforfølgning af lovovertrædelser
- e) AI-systemer, der er beregnet til at blive anvendt af retshåndhævende myndigheder eller på deres vegne til at forudsige forekomsten eller gentagelsen af en faktisk eller potentiel strafbar handling ud fra profilering af fysiske personer som omhandlet i artikel 3, stk. 4, i direktiv (EU) 2016/680 eller til at vurdere fysiske personers eller gruppers personlighedstræk og personlige egenskaber eller tidligere kriminelle adfærd
- f) AI-systemer, der er beregnet til at blive anvendt af retshåndhævende myndigheder eller på deres vegne til profilering af fysiske personer som omhandlet i artikel 3, stk. 4, i direktiv (EU) 2016/680 i forbindelse med afsløring, efterforskning eller retsforfølgning af lovovertrædelser.
- g) [udgår]

7. Migrationsstyring, asylforvaltning og grænsekontrol:

- a) AI-systemer, der er beregnet til at blive anvendt af kompetente offentlige myndigheder eller på deres vegne som polygrafer og lignende værktøjer eller til at påvise en fysisk persons følelsesmæssige tilstand
- b) AI-systemer, der er beregnet til at blive anvendt af kompetente offentlige myndigheder eller på deres vegne til at vurdere en risiko, herunder en sikkerhedsrisiko, en risiko for irregulær migration eller en sundhedsrisiko, som udgøres af en fysisk person, der har til hensigt at rejse ind i eller er indrejst i en medlemsstat

- c) [udgår]
- d) AI-systemer, der er beregnet til at blive anvendt af kompetente offentlige myndigheder eller på deres vegne til at behandle ansøgninger om asyl, visum og opholdstilladelser og hertil relaterede klager med henblik på at fastslå, om de fysiske personer, der ansøger, er berettigede.

8. Retspleje og demokratiske processer:

- a) AI-systemer, der er beregnet til at blive anvendt af retlige myndigheder eller på deres vegne med at fortolke fakta eller lovgivningen og anvende lovgivningen i konkrete, faktuelle sager.

BILAG IV

TEKNISK DOKUMENTATION, jf. artikel 11, stk. 1

Den tekniske dokumentation, der er omhandlet i artikel 11, stk. 1, skal som minimum indeholde følgende oplysninger, alt efter hvad der er relevant for det pågældende AI-system:

1. En generel beskrivelse af AI-systemet, herunder:
 - a) det tilsigtede formål, den eller de personer, der udvikler systemet, samt systemets dato og version
 - b) hvis det er relevant, hvordan AI-systemet interagerer eller kan bruges til at interagere med hardware eller software, der ikke er en del af selve AI-systemet
 - c) versionerne af relevant software eller firmware og eventuelle krav vedrørende opdatering
 - d) en beskrivelse af alle måder, hvorpå AI-systemet bringes i omsætning eller tages i brug (f.eks. som softwarepakke indlejret i hardware, som kan downloades, API osv.)
 - e) en beskrivelse af den hardware, som AI-systemet er beregnet til at køre på
 - f) hvis AI-systemet er komponent i produkter: fotografier eller illustrationer, der viser disse produkters eksterne karakteristika, mærkning og interne layout
 - g) brugsanvisning til brugeren og, hvis det er relevant, monteringsvejledning.
2. En detaljeret beskrivelse af elementerne i AI-systemet og af processen for dets udvikling, herunder:
 - a) de metoder og trin, der er brugt i udviklingen af AI-systemet, herunder, hvor det er relevant, anvendelse af forhåndstrænede systemer eller værktøjer leveret af tredjeparter, og hvordan disse er blevet anvendt, integreret eller ændret af udbyderen

- b) systemets konstruktionsspecifikationer, dvs. AI-systemets og algoritmernes generelle logik, navnlig de vigtigste designvalg, herunder begrundelser og antagelser, også med hensyn til personer eller grupper af personer, som systemet er beregnet til at blive anvendt på, de overordnede klassifikationsvalg, hvad systemet er designet til at optimere for og relevansen af de forskellige parametre, en beskrivelse af systemets forventede output samt beslutninger om eventuelle trade-offs i de tekniske løsninger, der er valgt for at opfylde kravene i afsnit III, kapitel 2
- c) en beskrivelse af systemarkitekturen, der forklarer, hvordan softwarekomponenterne bygger på eller tilføjes hinanden og integreres i den samlede anvendelse; de beregningsressourcer, der anvendes til at udvikle, træne, teste og validere AI-systemet
- d) hvis det er relevant, datakravene i form af datablade, der beskriver de anvendte træningsmetoder og -teknikker og de anvendte træningsdatasæt, herunder en generel beskrivelse af disse datasæt, oplysninger deres oprindelse, omfang og vigtigste karakteristika, hvordan dataene er indsamlet og udvalgt, mærkningsprocedurer (f.eks. for superviseret læring) og datarensningmetoder (f.eks. detektion af outliers)
- e) vurdering af de foranstaltninger til menneskeligt tilsyn, der er nødvendige i henhold til artikel 14, herunder en vurdering af de tekniske foranstaltninger, der er nødvendige for at lette brugernes fortolkning af AI-systemets output, jf. artikel 13, stk. 3, litra d)
- f) hvis det er relevant, en detaljeret beskrivelse af på forhånd fastlagte ændringer af AI-systemet og dets ydeevne sammen med alle relevante oplysninger vedrørende de tekniske løsninger, der er valgt for at sikre, at AI-systemet til stadighed opfylder de relevante krav i afsnit III, kapitel 2

- g) de anvendte validerings- og prøvningsprocedurer, herunder oplysninger om de anvendte validerings- og testdata og deres vigtigste karakteristika, parametre til måling af nøjagtighed, robusthed, cybersikkerhed og overholdelse af andre relevante krav i afsnit III, kapitel 2, herunder potentielt diskriminerende virkninger, samt testlogfiler og alle testrapporter, der er dateret og underskrevet af de ansvarlige personer, herunder med hensyn til forudbestemte ændringer som omhandlet i litra f).
3. Detaljerede oplysninger om AI-systemets funktion, samt overvågning og kontrol, navnlig med hensyn til dets kapacitet og begrænsninger i ydeevne, herunder nøjagtighedsgraden for specifikke personer eller grupper af personer, som systemet er beregnet til at blive anvendt på, og det samlede forventede nøjagtighedsniveau i forhold til det tilsigtede formål, de forventede utilsigtede resultater og kilder til risici for sundhed og sikkerhed, grundlæggende rettigheder og forskelsbehandling i lyset af AI-systemets tilsigtede formål, foranstaltningerne til menneskeligt tilsyn i overensstemmelse med artikel 14, herunder de tekniske foranstaltninger, der er indført for at lette brugernes fortolkning af AI-systemets output, samt specifikationer for inputdata, hvis det er relevant
4. en detaljeret beskrivelse af risikostyringssystemet i overensstemmelse med artikel 9
5. en beskrivelse af relevante ændringer, som udbyderen foretager af systemet i løbet af dets livscyklus
6. en liste over de helt eller delvis anvendte harmoniserede standarder, hvis referencer er offentliggjort i Den Europæiske Unions Tidende, samt, hvis disse harmoniserede standarder ikke er blevet anvendt, detaljerede beskrivelser af de løsninger, der er anvendt for at opfylde kravene, der er fastsat i afsnit III, kapitel 2, herunder en liste over andre relevante tekniske specifikationer, som er anvendt
7. en kopi af EU-overensstemmelseserklæringen
8. en detaljeret beskrivelse af det system, der er indført til evaluering af AI-systemets ydeevne, efter at systemet er bragt i omsætning, jf. artikel 61, herunder planen for overvågning efter omsætningen, jf. artikel 61, stk. 3.

BILAG V

EU-OVERENSSTEMMELSESERKLÆRING

EU-overensstemmelseserklæringen, jf. artikel 48, skal indeholde følgende oplysninger:

1. AI-systemets navn, type og enhver yderligere entydig reference, der gør det muligt at identificere og spore AI-systemet
2. udbyderens navn og adresse eller, hvis det er relevant, den autoriserede repræsentants navn og adresse
3. en erklæring om, at EU-overensstemmelseserklæringen udstedes på udbyderens ansvar
4. en erklæring om, at det pågældende AI-system er i overensstemmelse med denne forordning og eventuelt med al anden relevant EU-lovgivning, der fastsætter bestemmelser om udstedelse af en EU-overensstemmelseserklæring
5. referencer til de relevante anvendte harmoniserede standarder eller referencer til anden fælles specifikation, som der erklæres overensstemmelse med
6. hvis det er relevant, navnet og identifikationsnummeret på det bemyndigede organ, en beskrivelse af den gennemførte overensstemmelsesvurderingsprocedure og identifikation af det udstedte certifikat
7. udstedelsessted og -dato for erklæringen, navn og stilling på den person, der har underskrevet den, samt en angivelse af, for hvem og på hvis vegne vedkommende har underskrevet, og underskrift.

BILAG VI
PROCEDURER FOR OVERENSSTEMMELSESVURDERING BASERET PÅ INTERN
KONTROL

1. Proceduren for overensstemmelsesvurdering baseret på intern kontrol er overensstemmelsesvurderingsproceduren beskrevet i punkt 2-4
2. Udbyderen kontrollerer, at det etablerede kvalitetsstyringssystem er i overensstemmelse med kravene i artikel 17.
3. Udbyderen undersøger oplysningerne i den tekniske dokumentation med henblik på at vurdere, hvorvidt AI-systemet opfylder de relevante væsentlige krav i afsnit III, kapitel 2.
4. Udbyderen kontrollerer også, at design- og udviklingsprocessen for AI-systemet og dets overvågning efter omsætningen, jf. artikel 61, er i overensstemmelse med den tekniske dokumentation.

BILAG VII
OVERENSSTEMMELSE BASERET PÅ VURDERING AF
KVALITETSSTYRINGSSYSTEMET OG PÅ VURDERING AF TEKNISK
DOKUMENTATION

1. Indledning

Overensstemmelse baseret på vurdering af kvalitetsstyringssystemet og vurdering af den tekniske dokumentation er overensstemmelsesvurderingsproceduren beskrevet i punkt 2-5.

2. Oversigt

Det godkendte kvalitetsstyringssystem for udformning, udvikling og prøvning af AI-systemer i henhold til artikel 17 undersøges i overensstemmelse med punkt 3 og er underlagt den i punkt 5 omhandlede kontrol. AI-systemets tekniske dokumentation undersøges i overensstemmelse med punkt 4.

3. Kvalitetsstyringssystem

3.1. Udbyderens ansøgning skal omfatte:

- a) udbyderens navn og adresse og desuden udbyderens bemyndigede repræsentants navn og adresse, hvis ansøgningen indgives af denne
- b) listen over AI-systemer, der er omfattet af det samme kvalitetsstyringssystem
- c) den tekniske dokumentation for hvert AI-system, der er omfattet af det samme kvalitetsstyringssystem
- d) dokumentationen vedrørende kvalitetsstyringssystemet, som skal omfatte alle de aspekter, der er anført i artikel 17

- e) en beskrivelse af de procedurer, der er indført for at sikre, at kvalitetsstyringssystemet fortsat vil fungere hensigtsmæssigt og effektivt
- f) en skriftlig erklæring om, at samme ansøgning ikke er blevet indgivet til et andet bemyndiget organ.

3.2. Det bemyndigede organ vurderer kvalitetsstyringssystemet for at fastslå, om det opfylder kravene i artikel 17.

Afgørelsen meddeles udbyderen eller dennes bemyndigede repræsentant.

Meddelelsen skal indeholde resultaterne af vurderingen af kvalitetsstyringssystemet og en begrundelse for afgørelsen.

3.3. Det godkendte kvalitetsstyringssystem skal vedligeholdes af udbyderen, således at det forbliver hensigtsmæssigt og effektivt.

3.4. Enhver påtænkt ændring af det godkendte kvalitetsstyringssystem eller listen over AI-systemer, der er omfattet af dette, skal af udbyderen meddeles det bemyndigede organ.

Det bemyndigede organ vurderer de foreslåede ændringer og afgør, om det ændrede kvalitetsstyringssystem stadig opfylder de i punkt 3.2 omhandlede krav, eller om en fornyet vurdering er nødvendig.

Det bemyndigede organ meddeler udbyderen sin afgørelse. Meddelelsen skal indeholde resultaterne af undersøgelsen af de foreslåede ændringer og en begrundelse for afgørelsen.

4. Kontrol af den tekniske dokumentation

4.1. Ud over den i punkt 3 omhandlede ansøgning, skal udbyderen til det bemyndigede organ indsende en ansøgning om vurdering af den tekniske dokumentation vedrørende det AI-system, som denne agter at bringe i omsætning eller ibrugtage, og som er omfattet af det kvalitetsstyringssystem, der er omhandlet i punkt 3.

- 4.2. Ansøgningen skal indeholde:
- a) udbyderens navn og adresse
 - b) en skriftlig erklæring om, at samme ansøgning ikke er blevet indgivet til et andet bemyndiget organ
 - c) den i bilag IV omhandlede tekniske dokumentation.
- 4.3. Den tekniske dokumentation vurderes af det bemyndigede organ. Hvor det er relevant og begrænset til, hvad der er nødvendigt, for at det kan udføre sine opgaver, skal det bemyndigede organ have fuld adgang til de anvendte trænings-, validerings- og prøvningsdatasæt, herunder, hvor det er relevant og med forbehold af sikkerhedsforanstaltninger, via programmeringsgrænseflader for applikationer (API'er) eller andre relevante tekniske midler og værktøjer, der muliggør fjernadgang.
- 4.4. I forbindelse med vurderingen af den tekniske dokumentation kan det bemyndigede organ kræve, at udbyderen fremlægger yderligere dokumentation eller udfører yderligere prøvninger for at muliggøre en korrekt vurdering af AI-systemets overensstemmelse med kravene i afsnit III, kapitel 2. Hvis det bemyndigede organ ikke er tilfreds med de prøvninger, som udbyderen har foretaget, skal det bemyndigede organ selv foretage de nødvendige prøvninger direkte, hvis det er relevant.
- 4.5. De bemyndigede organer gives efter begrundet anmodning adgang til kildekoden for AI-systemet, og kun når følgende kumulative betingelser er opfyldt:
- a) Adgang til kildekode er nødvendig for at vurdere, om højrisiko-AI-systemet er i overensstemmelse med kravene i afsnit III, kapitel 2, og
 - b) prøvnings-/revisionsprocedurer og verificeringer på grundlag af data og dokumentation fra udbyderen er udtømt eller har vist sig at være utilstrækkelige.

- 4.6. Afgørelsen meddeles udbyderen eller dennes bemyndigede repræsentant. Meddelelsen skal indeholde resultaterne af vurderingen af den tekniske dokumentation og en begrundelse for afgørelsen.

Hvis AI-systemet opfylder kravene i afsnit III, kapitel 2, udsteder det bemyndigede organ et EU-vurderingscertifikat for teknisk dokumentation. Certifikatet skal indeholde udbyderens navn og adresse, undersøgelseskonklusionerne, eventuelle betingelser for dets gyldighed og de nødvendige data til identifikation af AI-systemet.

Certifikatet og bilagene hertil skal indeholde alle relevante oplysninger, der gør det muligt at vurdere AI-systemets opfyldelse af kravene, herunder, hvis det er relevant, kontrol under brug.

Hvis AI-systemet ikke opfylder kravene i afsnit III, kapitel 2, afviser det bemyndigede organ at udstede et EU-vurderingscertifikat for teknisk dokumentation og oplyser ansøgeren herom og giver en detaljeret begrundelse for afslaget.

Hvis AI-systemet ikke opfylder kravet vedrørende de data, der anvendes til at træne det, skal AI-systemet gentrænes, inden der ansøges om en ny overensstemmelsesvurdering. I dette tilfælde skal det bemyndigede organs begrundede afgørelse om afslag på udstedelse af et EU-vurderingscertifikat for teknisk dokumentation indeholde specifikke betragtninger om kvaliteten af de data, der er anvendt til at træne AI-systemet, navnlig om årsagerne til, at systemet ikke opfylder kravene.

- 4.7. Enhver ændring af AI-systemet, der kan påvirke AI-systemets opfyldelse af kravene eller systemets tilsigtede formål, skal godkendes af det bemyndigede organ, der udstedte EU-vurderingscertifikatet for teknisk dokumentation. Udbyderen skal underrette det bemyndigede organ om sin hensigt om at indføre nogen af ovennævnte ændringer, eller hvis denne på anden måde bliver opmærksom på forekomsten af sådanne ændringer. Det bemyndigede organ vurderer de påtænkte ændringer og afgør, om de påtænkte ændringer kræver en ny overensstemmelsesvurdering i henhold til artikel 43, stk. 4, eller om de kan behandles ved hjælp af et tillæg til EU-vurderingscertifikatet for teknisk dokumentation. I sidstnævnte tilfælde vurderer det bemyndigede organ ændringerne, underretter udbyderen om sin afgørelse og udsteder, såfremt ændringerne godkendes, et tillæg til EU-vurderingscertifikatet for teknisk dokumentation til udbyderen.
5. Overvågning af det godkendte kvalitetsstyringssystem
- 5.1. Formålet med det tilsyn, der udføres af det bemyndigede organ, der er omhandlet i punkt 3, er at sikre, at udbyderen behørigt opfylder vilkårene og betingelserne i det godkendte kvalitetsstyringssystem.
- 5.2. Med henblik på vurdering skal udbyderen give det bemyndigede organ adgang til de lokaler, hvor udformningen, udviklingen og prøvningen af AI-systemerne finder sted. Udbyderen skal yderligere give det bemyndigede organ alle nødvendige oplysninger.
- 5.3. Det bemyndigede organ aflægger jævnligt kontrolbesøg for at sikre, at udbyderen vedligeholder og anvender kvalitetsstyringssystemet, og det udsteder en kontrolrapport til udbyderen. I forbindelse med disse kontrolbesøg kan det bemyndigede organ foretage yderligere prøvninger af de AI-systemer, for hvilke der er udstedt et EU-vurderingscertifikat for teknisk dokumentation.

BILAG VIII

OPLYSNINGER, DER SKAL INDSENDES VED REGISTRERING AF OPERATØRER OG HØJRIKIO-AI-SYSTEMER, JF. ARTIKEL 51

Udbydere, bemyndigede repræsentanter og brugere, der er offentlige myndigheder, agenturer eller organer, indsender de oplysninger, der er omhandlet i del I. Udbydere eller, hvor det er relevant, bemyndigede repræsentanter sikrer, at oplysningerne om deres højrisko-AI-systemer, jf. del II, punkt 1-11, er fuldstændige, korrekte og ajourførte. Oplysningerne i del II, punkt 12, genereres automatisk af databasen.

Del I. Oplysninger om operatører (efter operatørernes registrering)

- 1. Type operatør (udbyder, bemyndiget repræsentant eller bruger)
 - 1. udbyderens navn, adresse og kontaktoplysninger
 - 2. hvis oplysninger forelægges af en anden person på vegne af operatøren, denne persons navn, adresse og kontaktoplysninger.

Del II. Oplysninger vedrørende højrisko-AI-systemet

- 1. udbyderens navn, adresse og kontaktoplysninger
- 2. den bemyndigede repræsentants navn, adresse og kontaktoplysninger, hvis det er relevant
- 3. AI-systemets handelsnavn og enhver yderligere entydig reference, der gør det muligt at identificere og spore AI-systemet
- 4. beskrivelse af det tilsigtede formål med AI-systemet
- 5. AI-systemets status (i omsætning/i drift, ikke længere i omsætning/i drift, tilbagekaldt)
- 6. type, nummer og udløbsdato for det certifikat, der er udstedt af det bemyndigede organ, samt navn eller identifikationsnummer på det pågældende bemyndigede organ, hvis det er relevant

7. en scannet kopi af det i punkt 6 omhandlede certifikat, hvis det er relevant
8. medlemsstater, hvor AI-systemet bringes i omsætning eller er bragt i omsætning, ibrugtages eller er taget i brug, gøres tilgængeligt eller er tilgængeligt i Unionen
9. en kopi af den i artikel 48 omhandlede EU-overensstemmelseserklæring
10. brugsanvisninger i elektronisk form,
11. URL for yderligere oplysninger (valgfrit)
12. brugernes navn, adresse og kontaktoplysninger.

BILAG VIIIa

OPLYSNINGER, DER SKAL FORELÆGGES VED REGISTRERING AF HØJRISIKO-AI-SYSTEMER ANFØRT I BILAG III I FORBINDELSE MED PRØVNING UNDER FAKTISKE FORHOLD I OVERENSSTEMMELSE MED ARTIKEL 54A

Følgende oplysninger skal forelægges og derefter holdes ajourført med hensyn til prøvning under faktiske forhold, der registreres i overensstemmelse med artikel 54a:

1. det EU-dækkende unikke individuelle identifikationsnummer for prøvningen under faktiske forhold
2. navn og kontaktoplysninger på udbyderen eller den potentielle udbyder og de brugere, der er involveret i prøvningen under faktiske forhold
3. en kort beskrivelse af AI-systemet, dets tilsigtede formål og andre oplysninger, der er nødvendige for at identificere systemet
4. et resumé af de vigtigste karakteristika ved planen for prøvning under faktiske forhold
5. Oplysninger om suspendering eller afslutning af prøvningen under faktiske forhold.

BILAG IX
**EU-LOVGIVNING OM STORE IT-SYSTEMER INDEN FOR OMRÅDET MED FRIHED,
SIKKERHED OG RETFÆRDIGHED**

1. Schengeninformationssystemet

- a) Europa-Parlamentets og Rådets forordning (EU) 2018/1860 af 28. november 2018 om brug af Schengeninformationssystemet i forbindelse med tilbagesendelse af tredjelandsstatsborgere med ulovligt ophold (EUT L 312 af 7.12.2018, s. 1)
- b) Europa-Parlamentets og Rådets forordning (EU) 2018/1861 af 28. november 2018 om oprettelse, drift og brug af Schengeninformationssystemet (SIS) på området ind- og udrejsekontrol, om ændring af konventionen om gennemførelse af Schengenaftalen og om ændring og ophævelse af forordning (EF) nr. 1987/2006 (EUT L 312 af 7.12.2018, s. 14)
- c) Europa-Parlamentets og Rådets forordning (EU) 2018/1862 af 28. november 2018 om oprettelse, drift og brug af Schengeninformationssystemet (SIS) på området politisamarbejde og strafferetligt samarbejde, om ændring og ophævelse af Rådets afgørelse 2007/533/RIA og om ophævelse af Europa-Parlamentets og Rådets forordning (EF) nr. 1986/2006 og Kommissionens afgørelse 2010/261/EU (EUT L 312 af 7.12.2018, s. 56).

2. Visuminformationssystemet

- a) Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om ændring af forordning (EF) nr. 767/2008, forordning (EF) nr. 810/2009, forordning (EU) 2017/2226, forordning (EU) 2016/399, forordning XX/2018 [forordningen om interoperabilitet] og beslutning 2004/512/EF og om ophævelse af Rådets afgørelse 2008/633/RIA – COM(2018) 302 final. Ajourføres, når forordningen er vedtaget (april/maj 2021) af medlovgiverne.

3. Eurodac

- a) Ændret forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om oprettelse af "Eurodac" til sammenligning af biometriske oplysninger med henblik på en effektiv anvendelse af forordning (EU) XXX/XXX [forordningen om asylforvaltning og migrationsstyring] og forordning (EU) XXX/XXX [genbosætningsforordningen], identificering af en tredjelandstatsborger eller en statsløs person med ulovligt ophold og om medlemsstaternes retshåndhævende myndigheders og Europols adgang til at indgive anmodning om sammenligning med Eurodacoplysninger med henblik på retshåndhævelse og om ændring af forordning (EU) 2018/1240 og (EU) 2019/818 – COM(2020) 614 final.

4. Ind- og udrejsesystemet

- a) Europa-Parlamentets og Rådets forordning (EU) 2017/2226 af 30. november 2017 om oprettelse af et ind- og udrejsesystem til registrering af ind- og udrejseoplysninger og oplysninger om nægtelse af indrejse vedrørende tredjelandstatsborgere, der passerer medlemsstaternes ydre grænser, om fastlæggelse af betingelserne for adgang til ind- og udrejsesystemet til retshåndhævelsesformål og om ændring af konventionen om gennemførelse af Schengenaftalen og forordning (EF) nr. 767/2008 og (EU) nr. 1077/2011 (EUT L 327 af 9.12.2017, s. 20).

5. Det europæiske system vedrørende rejseinformation og rejsetilladelse

- a) Europa-Parlamentets og Rådets forordning (EU) 2018/1240 af 12. september 2018 om oprettelse af et europæisk system vedrørende rejseinformation og rejsetilladelse (ETIAS) og om ændring af forordning (EU) nr. 1077/2011, (EU) nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 og (EU) 2017/2226 (EUT L 236 af 19.9.2018, s. 1)
- b) Europa-Parlamentets og Rådets forordning (EU) 2018/1241 af 12. september 2018 om ændring af forordning (EU) 2016/794 med henblik på oprettelse af et europæisk system vedrørende rejseinformation og rejsetilladelse (ETIAS) (EUT L 236 af 19.9.2018, s. 72).

6. Det europæiske informationssystem vedrørende strafferegistre for statsborgere i tredjelande og statsløse
- a) Europa-Parlamentets og Rådets forordning (EU) 2019/816 af 17. april 2019 om oprettelse af et centralt system til bestemmelse af, hvilke medlemsstater der ligger inde med oplysninger om straffedomme afsagt over tredjelandsstatsborgere og statsløse personer (ECRIS-TCN) for at supplere det europæiske informationssystem vedrørende strafferegistre, og om ændring af forordning (EU) 2018/1726 (EUT L 135 af 22.5.2019, s. 1).
7. Interoperabilitet
- a) Europa-Parlamentets og Rådets forordning (EU) 2019/817 af 20. maj 2019 om fastsættelse af en ramme for interoperabilitet mellem EU-informationssystemer vedrørende grænser og visum (EUT L 135 af 22.5.2019, s. 27)
- b) Europa-Parlamentets og Rådets forordning (EU) 2019/818 af 20. maj 2019 om fastsættelse af en ramme for interoperabilitet mellem EU-informationssystemer vedrørende politisamarbejde og retligt samarbejde, asyl og migration (EUT L 135 af 22.5.2019, s. 85).
-