Tidende
av Den europeiske union

DA
L-serien

2024/1689

12.7.2024

EUROPAPARLAMENTETS OG RÅDETS FORORDNING (EU) NR. 2024/1689

av 13. juni 2024

om fastsettelse av harmoniserte regler om kunstig intelligens og om endring av forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2019/2144 og Direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (lov om kunstig intelligens)

(EØS-relevant tekst)

DEN EUROPEISKE PArLEMENTET OG rÅDET FOR DEN EUROPEISKE UNION,

under henvisning til traktaten om Den europeiske unions virkemåte, særlig artikkel 16 og 114, under henvisning til forslag fra

Europakommisjonen, og

etter at utkastet til rettsakt er oversendt til de nasjonale parlamentene,

under henvisning til uttalelse fra Den europeiske økonomiske og sosiale komité ([1]), under

henvisning til uttalelse fra Den europeiske sentralbank ([2])

under henvisning til uttalelse fra Regionkomiteen ([3]), I henhold til den ordinære

regelverksprosessen ([4]), og ut fra følgende betraktninger

(1) Formålet med denne forordning er å forbedre det indre markeds virkemåte ved å fastsette en ensartet rettslig ramme, særlig for utvikling, markedsføring, ibruktaking og bruk av systemer for kunstig intelligens (aI-systemer) i Unionen, I samsvar med Unionens verdier, å fremme innføringen av menneskesentrert og pålitelig kunstig intelligens (AI), samtidig som det sikres et høyt nivå av beskyttelse av helse, sikkerhet, grunnleggende rettigheter som nedfelt i Den europeiske unions pakt om grunnleggende rettigheter ("pakten"), herunder demokrati, rettsstatsprinsipper og miljøvern, å beskytte mot skadelige virkninger av aI-systemer i Unionen og å støtte innovasjon. Denne forordningen sikrer fri bevegelighet over landegrensene FOR KI-BASERTE varer og tjenester, og hindrer dermed medlemsstatene i å innføre restriksjoner på utvikling, markedsføring og bruk av KI-systemer, med mindre det er uttrykkelig tillatt i henhold til denne forordningen.

(2) Denne forordning bør anvendes i samsvar med Unionens verdier, slik de er nedfelt i pakten, og legge til rette for beskyttelse av fysiske personer, foretak, demokrati, rettsstatsprinsipper og miljøvern, samtidig som den fremmer innovasjon og sysselsetting og gjør Unionen til en ledende aktør når det gjelder å ta i bruk pålitelig AI.

(3) aI-systemer kan enkelt tas i bruk I en lang rekke sektorer av økonomien og mange deler av samfunnet, på tvers av landegrensene, og kan lett sirkulere i hele unionen. Enkelte medlemsstater har allerede undersøkt muligheten for å vedta nasjonale regler for å sikre at AI er pålitelige og sikre og utvikles og brukes i samsvar med forpliktelsene knyttet til grunnleggende rettigheter. ulike nasjonale regler kan føre til fragmentering av det indre marked og redusere rettssikkerheten for aktører som utvikler, importerer eller bruker aI-systemer. Det bør derfor sikres ET konsekvent og høyt beskyttelsesnivå i hele Unionen for å oppnå pålitelig AI, samtidig som avvik som hindrer fri omsetning, innovasjon, utplassering og utbredelse av AI-SYSTEMER og tilknyttede produkter og tjenester i det indre marked, bør forhindres ved å fastsette ensartede forpliktelser for operatører og

(1) EUT C 517 av 22.12.2021, s. 56.
(2) EUT C 115 av 11.3.2022, s. 5.
(3) EUT C 97 av 28.2.2022, s. 60.
(4) Europaparlamentets holdning av 13. mars 2024 (ennå ikke offentliggjort i EUT) og Rådets beslutning av 21. mai 2024.

som garanterer et ensartet vern af tvingende allmenne hensyn og af personers rettigheder i hele indre marked på grundlag af artikel 114 i traktaten om Den europæiske unions virkemåde (TEUV). I den udstrækning denne forordning indeholder særlige regler om vern af fysiske personer med hensyn til behandling af personoplysninger som gjelder begrensninger bruken AV KI-systemer for biometrisk fjernidentifikasjon med henblikk på rettshåndhevelse, I bruken AV KI-SYSTEMER for risikovurderinger av fysiske personer med henblikk på rettshåndhevelse og i bruken AV KI-systemer for biometrisk kategorisering med henblikk på rettshåndhevelse, bør denne forordning, i den udstrækning det gjelder disse særlige reglene, baseres på artikel 16 i TEUV. I lys disse særreglene og henvisningen til artikel 16 i TEUV er det hensiktsmessig å rådføre seg med Det europæiske personvernråd.

(4) KI er en teknologi I rask utvikling som bidrar til en lang rekke økonomiske, miljømessige og samfunnsmessige fordeler i hele spekteret av bransjer og samfunnsaktiviteter. Ved å forbedre prediksjon, optimalisere drift og ressursallokering og personalisere digitale løsninger som er tilgjengelige for enkeltpersoner og organisasjoner, kan bruk av AI gi viktige konkurransefortrinn for virksomheter og støtte opp om sosialt og miljømessig gunstige resultater, for eksempel innen helsevesen, landbruk, mattrygghet, utdanning og opplæring, media, idrett, kultur, infrastrukturforvaltning, energi, transport og logistikk, offentlige tjenester, sikkerhet, rettsvesen, ressurs- og energieffektivitet, miljøovervåking, bevaring og gjenoppretting av biologisk mangfold og økosystemer samt avbøting av og tilpasning til klimaendringer.

(5) Samtidig kan AI, avhengig av omstendighetene knyttet til den spesifikke anvendelsen, bruken og det teknologiske utviklingsnivået, medføre risiko og skade på allmenne interesser og grunnleggende rettigheter som er beskyttet av unionsretten. Slik skade kan være materiell eller immateriell, herunder fysisk, psykologisk, samfunnsmessig eller økonomisk skade.

(6) Med tanke på den store innvirkningen KI kan ha på samfunnet og behovet for å bygge tillit, er det avgjørende at KI og regelverket for den utvikles i samsvar med Unionens verdier, slik de er nedfelt i artikkel 2 i traktaten om Den europæiske union (TEU), de grunnleggende rettighetene og frihetene som er nedfelt i traktatene og, i henhold til artikkel 6 I TEU, pakten. Den skal være et verktøy for mennesker, med det endelige målet å øke menneskers velferd.

(7) For å sikre et konsekvent og høyt nivå for beskyttelse av allmennhetens interesser når det gjelder helse, sikkerhet og grunnleggende rettigheter, bør det fastsettes felles regler for høyrisikosystemer. Disse reglene bør være i samsvar med pakten, ikke-diskriminerende og i tråd med Unionens internasjonale handelsforpliktelser. De bør også ta hensyn til den europeiske erklæringen om digitale rettigheter og prinsipper for det digitale tiåret og de etiske retningslinjene for pålitelig kunstig intelligens fra høynivåekspertgruppen for kunstig intelligens (AI HLEG).

(8) Det er derfor nødvendig MED ET unionsregelverk som fastsetter harmoniserte regler om AI, for å fremme utvikling, bruk og utbredelse av AI i det indre marked, og som samtidig sikrer et høyt nivå av vern av allmenne interesser, helse og sikkerhet og vern av grunnleggende rettigheter, herunder demokrati, rettsstatsprinsipper og miljøvern, slik de er anerkjent og beskyttet i unionsretten. For å nå dette målet bør det fastsettes regler for markedsføring, IBRUKTAKING og bruk av visse AI-systemer, slik at det sikres at det indre marked fungerer smidig, og slik at disse systemene kan dra fordel av prinsippet om fri bevegelighet for varer og tjenester. Disse reglene bør være klare og robuste når det gjelder å beskytte grunnleggende rettigheter, støtte nye innovative løsninger, muliggjøre et europeisk økosystem av offentlige og private aktører som skaper aI-systemer i tråd med Unionens verdier og frigjøre potensialet i den digitale transformasjonen I alle regioner i UnionenVed å fastsette disse reglene samt tiltak til støtte for innovasjon med særlig fokus på små og mellomstore bedrifter (SMB-er), herunder oppstartsbedrifter, støtter denne forordningen målet om å fremme den europeiske menneskesentrerte tilnærmingen til aI og være en global leder i utviklingen av sikker, pålitelig og etisk aI, slik Det europeiske råd har uttalt på ([5]), og den sikrer beskyttelsen av etiske prinsipper, slik det ble uttrykkelig anmodet om av Europaparlamentet på ([6].)

(5) Det europeiske råd, Ekstraordinært møte i Det europeiske råd (1. og 2. oktober 2020) - Konklusjoner, EUCO 13/20, 2020, s. 6.

(6) Europaparlamentets resolusjon av 20. oktober 2020 med anbefalinger til Kommisjonen om en ramme for etiske aspekter ved kunstig intelligens, robotteknologi og beslektet teknologi, 2020/2012(INL).

(9) Harmoniserte regler for omsetning, ibruktaking og bruk av høyrisikosystemer bør fastsettes i samsvar med europaparlaments- og rådsforordning (EF) nr. 765/2008 ((7)), europaparlaments- og rådsbeslutning nr. 768/2008/EF (8) og europaparlaments- og rådsforordning (EU) 2019/1020 (9) ("den nye rettslige rammen"). De harmoniserte reglene fastsatt i denne forordning bør få anvendelse på tvers av sektorer og bør, i tråd med det nye rettslige rammeverket, ikke berøre gjeldende unionsrett, særlig om databeskyttelse, forbrukervern, grunnleggende rettigheter, sysselsetting og vern av arbeidstakere samt produktsikkerhet, som denne forordning utfyller. Som en konsekvens av dette forblir alle rettigheter og rettsmidler fastsatt i slik unionsrett for forbrukere og andre personer som KI-systemer kan ha en negativ innvirkning på, herunder med hensyn til kompensasjon for eventuelle skader i henhold til rådsdirektiv 85/374/EØF ((10)), upåvirket og fullt ut anvendelige. Når det gjelder sysselsetting og vern av arbeidstakere, bør denne forordning derfor ikke berøre unionsretten om sosialpolitikk og nasjonal arbeidsrett, i samsvar med unionsretten, om ansettelses- og arbeidsvilkår, herunder helse og sikkerhet på arbeidsplassen og forholdet mellom arbeidsgivere og arbeidstakere. Denne forordning bør heller ikke berøre utøvelsen av grunnleggende rettigheter som er anerkjent i medlemsstatene og på unionsplan, herunder retten eller friheten til å streike eller til å treffe andre tiltak som omfattes av de særlige ordningene for forholdet mellom partene i arbeidslivet i medlemsstatene, samt retten til å forhandle, inngå og håndheve tariffavtaler eller til å treffe kollektive tiltak i samsvar med nasjonal lovgivning. Denne forordning bør ikke berøre bestemmelsene som tar sikte på å forbedre arbeidsvilkårene i plattformarbeid, og som er fastsatt i et europaparlaments- og rådsdirektiv om forbedring av arbeidsvilkårene i plattformarbeid. Videre tar denne forordning sikte på å styrke effektiviteten av slike eksisterende rettigheter og rettsmidler ved å fastsette særlige krav og forpliktelser, herunder med hensyn til gjennomsiktighet, teknisk dokumentasjon og journalføring AV AI-systemer. Videre bør forpliktelsene som pålegges ulike aktører som er involvert i aI-verdikjeden i henhold til denne forordning, få anvendelse uten det berører nasjonal lovgivning, i samsvar med , med den virkning at bruken av visse aI-systemer begrenses når slik lovgivning faller utenfor denne forordnings virkeområde eller forfølger andre legitime mål av allmenn interesse enn dem som forfølges ved denne forordning. For eksempel bør nasjonal arbeidsrett og lovgivning om vern av mindreårige, dvs. personer under 18 år, idet det tas hensyn til UNCRC General Comment No 25 (2021) on children's rights in relation to the digital environment, I den grad de ikke er spesifikke for KI-systemer og forfølger andre legitime mål av allmenn interesse, ikke påvirkes av denne forordning.

(10) Den grunnleggende retten til vern av personopplysninger er særlig ivaretatt i europaparlaments- og rådsforordningene (EU) 2016/679 ((11)) (12) og (EU) 2018/1725 og europaparlaments- og rådsdirektiv (EU) 2016/680 (13). Europaparlamentets og Rådets direktiv 2002/58/EF (14) beskytter i tillegg privatlivets fred og kommunikasjonshemmeligheter, blant annet ved å fastsette vilkår for lagring av personopplysninger og andre data i, og tilgang fra, terminalutstyr. Disse unionsrettsaktene danner grunnlaget for en bærekraftig og ansvarlig databehandling, også når datasettene omfatter en blanding av personopplysninger og andre opplysninger. Denne forordningen søker ikke å påvirke anvendelsen av eksisterende unionsrett som regulerer behandling av personopplysninger, herunder oppgavene og fullmaktene til de uavhengige tilsynsmyndighetene som har kompetanse til å overvåke overholdelsen av disse rettsaktene. Den berører heller ikke forpliktelsene til leverandører og utbyggere AV KI-systemer i deres rolle som behandlingsansvarlige eller databehandlere som følger av unionsretten eller nasjonal rett om vern av personopplysninger, i den grad utformingen, utviklingen eller bruken av KI-systemer innebærer behandling av personopplysninger. Det er også hensiktsmessig å presisere at de registrerte fortsatt nyter godt av alle

(7) Europaparlaments- og rådsforordning (EF) nr. 765/2008 av 9. juli 2008 om fastsettelse av kravene til akkreditering og om oppheving av forordning (EØF) nr. 339/93 (EUT L 218 av 13.8.2008, s. 30).

(8) Europaparlaments- og rådsbeslutning nr. 768/2008/EF av 9. juli 2008 om felles rammer for markedsføring av produkter og om opphevelse av RÅDSBESLUTNING 93/465/EØF (EUT L 218 av 13.8.2008, s. 82).

(9) Europaparlaments- og rådsforordning (EU) 2019/1020 av 20. juni 2019 om markedstilsyn og samsvar for produkter og om endring av direktiv 2004/42/EF og forordning (EF) nr. 765/2008 og (EU) nr. 305/2011 (EUT L 169 av 25.6.2019, s. 1).

(10) Rådets direktiv 85/374/EØF av 25. juli 1985 om tilnærming av medlemsstatenes lover og forskrifter om produktansvar (EFT L 210 av 7.8.1985, s. 29).

(11) Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger og om oppheving av direktiv 95/46/EF (generell forordning om databeskyttelse) (EUT L 119 av 4.5.2016, s. 1).

(12) Europaparlaments- og rådsforordning (EU) 2018/1725 av 23. oktober 2018 om vern av fysiske personer i forbindelse med behandling av personopplysninger i Unionens institusjoner, organer, kontorer og byråer og om fri utveksling av slike opplysninger, og om oppheving av forordning (EF) nr. 45/2001 og beslutning nr. 1247/2002/EF (EUT L 295 av 21.11.2018, s. 39).

(13) Europaparlaments- og rådsdirektiv (EU) 2016/680 av 27. april 2016 om vern av fysiske personer i forbindelse med kompetente myndigheters behandling av personopplysninger for å forebygge, etterforske, avsløre eller straffeforfølge straffbare handlinger eller fullbyrde strafferettslige sanksjoner, og om fri utveksling av slike opplysninger, og om oppheving av Rådets rammeavgjørelse 2008/977/JHA (EUT L 119 av 4.5.2016, s. 89).

(14) Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om av og vern av privatlivets fred i den elektroniske kommunikasjonssektoren (direktiv om personvern og elektronisk kommunikasjon) (EFT L 201 av 31.7.2002, s. 37).

rettigheter og garantier som er gitt dem i henhold til unionsretten, herunder rettighetene knyttet til utelukkende automatisert individuell beslutningstaking, herunder profilering. Harmoniserte regler for markedsføring, og bruk AV KI-systemer som er etablert i henhold til denne forordning, bør legge til rette for en effektiv gjennomføring og gjøre det for de registrerte å utøve sine rettigheter og andre rettsmidler som er garantert i henhold til unionsretten om vern av personopplysninger og andre grunnleggende rettigheter.

(11) Denne forordning bør ikke berøre bestemmelsene om erstatningsansvar for tilbydere av formidlingstjenester som fastsatt i europaparlaments- og rådsforordning (EU) 2022/2065 ([15])

(12) Begrepet "aI-system" i denne forordning bør defineres klart og bør være nært knyttet til arbeidet i internasjonale organisasjoner som arbeider med AI, for å sikre rettssikkerhet, legge til rette for internasjonal konvergens og bred aksept, samtidig som det gir fleksibilitet til å ta hensyn til den raske teknologiske utviklingen på dette området. Videre bør definisjonen baseres på nøkkelegenskaper AI-SYSTEMER som skiller dem fra enklere tradisjonelle programvaresystemer eller programmeringsmetoder, og den bør ikke omfatte systemer som er basert på regler som utelukkende er definert AV fysiske personer for automatisk å utføre operasjoner. Denne evnen til å utlede refererer til prosessen med å oppnå , for eksempel spådommer, innhold, anbefalinger eller beslutninger, som kan påvirke fysiske og virtuelle miljøer, og til AI-SYSTEMERS evne til å utlede modeller eller algoritmer, eller begge deler, fra inndata eller data. Teknikkene som muliggjør slutninger når man bygger et aI-system, omfatter maskinlæringsmetoder som lærer av data hvordan man oppnår bestemte mål, og logikk- og kunnskapsbaserte metoder som utleder slutninger fra kodet kunnskap eller symbolsk representasjon av oppgaven som skal løses. Et KI-system kan utlede mer enn bare grunnleggende databehandling ved å muliggjøre læring, resonnering eller modellering. Begrepet "maskinbasert" viser til det faktum at aI-systemer kjører på maskiner. Henvisningen til eksplisitte eller implisitte mål understreker at aI-systemer kan operere i henhold til eksplisitt definerte mål eller implisitte mål. Målene for aI-systemet kan være forskjellige fra det tiltenkte formålet med aI-systemet i en bestemt kontekst. I denne forordningen skal omgivelser forstås som kontekster der aI-systemene opererer, mens utdata generert av aI-systemene gjenspeiler ulike funksjoner som aI-systemene utfører, og omfatter prediksjoner, innhold, anbefalinger eller beslutninger. aI-systemer er utformet for å operere med varierende grad av autonomi, noe som betyr at de har en viss grad av uavhengighet av menneskelig inngripen og evne til å operere uten menneskelig inngripen. Tilpasningsdyktigheten som et AI-SYSTEM kan ha etter at det er tatt i bruk, refererer til selvlærende evner som gjør at systemet kan endre seg mens det ER I bruk. kan brukes på frittstående basis eller som en komponent i et produkt, uavhengig av om systemet er fysisk integrert i produktet (innebygd) eller om det tjener produktets funksjonalitet uten å være integrert i det (ikke innebygd).

(13) Begrepet "utplasserer" i denne forordning bør tolkes som enhver fysisk eller juridisk person, herunder en offentlig myndighet, et byrå eller et annet organ, som bruker et aI-system under sin myndighet, unntatt når aI-systemet brukes i forbindelse med en personlig, ikke-profesjonell aktivitet. avhengig av typen aI-system kan bruken av systemet berøre andre personer enn utplassøren.

(14) Begrepet "biometriske opplysninger" som brukes i denne forordning, bør tolkes i lys av begrepet biometriske opplysninger som definert i artikkel 4 nr. 14 i forordning (EU) 2016/679, artikkel 3 nr. 18 i forordning (EU) 2018/1725 og artikkel 3 nr. 13 i direktiv (EU) 2016/680. Biometriske data kan brukes til autentisering, identifisering eller kategorisering av fysiske personer og å gjenkjenne følelser hos fysiske personer.

(15) Begrepet "biometrisk identifikasjon" som det vises til i denne forordning bør defineres som automatisert gjenkjenning av fysiske, fysiologiske og atferdsmessige menneskelige kjennetegn, f.eks. ansikt, øyebevegelser, kroppsform, stemme, prosodi, ganglag, kroppsholdning, hjertefrekvens, blodtrykk, lukt og tastetrykk, med det formål å fastslå en persons identitet ved å sammenligne biometriske data om denne personen med lagrede biometriske data om enkeltpersoner i en referansedatabase, uavhengig av om personen har gitt sitt samtykke eller ikke. Dette omfatter IKKE AI-systemer som skal brukes til biometrisk verifisering, herunder autentisering, hvis eneste formål er å bekrefte at en bestemt fysisk person er den personen han hun utgir seg for å være, og å bekrefte identiteten til en fysisk person med det ene formål å få tilgang til en tjeneste, låse opp en enhet eller få sikkerhetstilgang til lokaler.

([15]) Europaparlaments- og rådsforordning (EU) 2022/2065 av 19. oktober 2022 om et indre marked for digitale tjenester og om endring av direktiv 2000/31/EF (rettsakt om digitale tjenester) (EUT L 277 av 27.10.2022, s. 1).

(16) Begrepet "biometrisk kategorisering" som det vises til i denne forordning, bør defineres som inndeling av fysiske personer i bestemte kategorier på grunnlag av deres biometriske opplysninger. Slike spesifikke kategorier kan være knyttet til aspekter som kjønn, alder, hårfarge, ø, tatoveringer, adferds- eller personlighetstrekk, språk, religion, tilhørighet til en nasjonal minoritet, seksuell eller politisk orientering. Dette omfatter ikke biometriske kategoriseringssystemer som er en ren tilleggsfunksjon som er uløselig knyttet til en annen kommersiell tjeneste, noe som betyr at funksjonen av objektive tekniske grunner ikke kan brukes uten hovedtjenesten, og at integreringen denne funksjonen eller funksjonaliteten ikke er et middel til å omgå anvendelsen av reglene i denne forordningen. For eksempel kan filtre som kategoriserer ansikts- eller kroppstrekk som brukes på markedsplasser på nettet, utgjøre en slik tilleggsfunksjon, ettersom de bare kan brukes i forbindelse med hovedtjenesten, som består i å selge et produkt ved å gi forbrukeren mulighet til å forhåndsvise hvordan produktet vises på ham eller henne selv og hjelpe forbrukeren til å treffe en kjøpsbeslutning. Filtre som brukes på sosiale nettverkstjenester på nettet, og som kategoriserer ansikts- eller kroppstrekk for å gjøre det mulig for brukerne å legge til eller endre bilder eller videoer, kan også anses å være en tilleggsytelse, ettersom slike filtre ikke kan brukes uten at hovedtjenesten til de sosiale nettverkstjenestene består i deling av innhold på nettet.

(17) Begrepet "fjernstyrt biometrisk " som det vises til I denne forordning, bør defineres funksjonelt som ET AI-system beregnet på identifisering av fysiske personer uten deres aktive , vanligvis på avstand, gjennom sammenligning av en persons biometriske data med de biometriske dataene i en referansedatabase, uavhengig av hvilken teknologi, prosess eller type biometriske data som brukes. Slike systemer for ekstern biometrisk identifikasjon brukes vanligvis til å oppfatte flere personer eller deres atferd samtidig for å gjøre det vesentlig lettere å identifisere fysiske personer uten deres aktive medvirkning. Dette utelukker AI-systemer som er beregnet på å brukes til biometrisk verifisering, som omfatter autentisering, hvis eneste formål er å bekrefte at en bestemt fysisk person er den personen han eller hun utgir seg for å være, og å bekrefte identiteten til en fysisk person med det ene formål å få tilgang til en tjeneste, låse opp en enhet eller få sikkerhetstilgang lokaler. Dette unntaket begrunnes med at slike systemer sannsynligvis vil ha mindre innvirkning på fysiske personers grunnleggende rettigheter sammenlignet med systemer for ekstern biometrisk identifikasjon, som kan brukes til behandling av biometriske opplysninger om et stort antall personer uten deres aktive medvirkning. Når det gjelder "sanntidssystemer", skjer innsamlingen av de biometriske dataene, sammenligningen og identifiseringen umiddelbart, nesten umiddelbart eller i alle fall uten vesentlig forsinkelse. I denne forbindelse bør det ikke være mulig å omgå reglene i denne forordning om "sanntids"-bruk AV de berørte AI-systemene ved å tillate mindre forsinkelser. Sanntidssystemer innebærer bruk av "live"- eller "nær-live"-materiale, for eksempel videoopptak, som genereres av et kamera eller annen enhet med lignende funksjonalitet. I "post"-systemer, derimot, er de biometriske dataene allerede tatt opp, og sammenligningen og identifiseringen skjer først etter en betydelig forsinkelse. Det dreier seg her om materiale, for eksempel bilder eller videoopptak generert av kameraer eller privat utstyr, som er generert før systemet tas i bruk med hensyn til de berørte fysiske personene.

(18) Begrepet "" som det vises TIL I denne forordning, bør defineres som ET AI-system som har til formål å identifisere eller utlede følelser eller intensjoner hos fysiske personer på grunnlag av deres biometriske data. Begrepet viser til følelser eller intensjoner som lykke, tristhet, sinne, overraskelse, avsky, forlegenhet, opphisselse, skam, forakt, tilfredshet og underholdning. Det omfatter ikke fysiske tilstander som smerte eller tretthet, for eksempel systemer som brukes til å detektere tretthetstilstanden til profesjonelle piloter eller sjåfører for å forebygge ulykker. Det omfatter heller ikke deteksjon av lett synlige uttrykk, gester eller bevegelser, med mindre de brukes til å identifisere eller utlede følelser. Slike uttrykk kan være enkle ansiktsuttrykk, for eksempel en rynke i pannen eller et smil, eller bevegelser, for eksempel bevegelser av hender, armer eller hode, eller kjennetegn ved en persons stemme, for eksempel en hevet stemme eller hvisking.

(19) I denne forordning bør begrepet "offentlig tilgjengelig sted" forstås som ethvert fysisk sted som er tilgjengelig for et ubestemt antall fysiske personer, uavhengig av om det aktuelle stedet er i privat eller offentlig eie, og uavhengig av hvilken aktivitet stedet kan brukes til, for eksempel til handel, for eksempel butikker, restauranter, kafeer; for tjenester, for eksempel banker, profesjonell virksomhet, servering; for sport, for eksempel svømmehaller, treningssentre, stadioner; for transport, for eksempel , t-bane- og jernbanestasjoner, flyplasser, transportmidler; for underholdning, for eksempel kinoer, teatre, museer, konsert- og konferansesaler; eller for fritid eller annet, for eksempel offentlige veier og plasser, parker, skoger, lekeplasser. Et område bør også klassifiseres som offentlig tilgjengelig dersom det, uavhengig av eventuelle kapasitets- eller sikkerhetsbegrensninger, er underlagt visse forhåndsbestemte vilkår som kan oppfylles av et ubestemt antall personer, for eksempel kjøp av billett eller transportbevis, forhåndsregistrering eller en viss alder. Derimot bør et område ikke anses for å være allment tilgjengelig dersom tilgangen er begrenset til bestemte og definerte fysiske personer gjennom enten unionsretten eller nasjonal rett som er direkte knyttet til offentlig sikkerhet eller trygghet, eller gjennom en klar manifestasjon av

av vilje fra den personen som har den relevante myndigheten over området. Den faktiske muligheten for adgang alene, for eksempel en ulåst dør eller en åpen port i et gjerde, innebærer ikke at området er offentlig tilgjengelig selv om det foreligger indikasjoner eller omstendigheter som tyder på det motsatte, f.eksskilt som forbyr eller begrenser adgangen. Bedrifts- og fabrikklokaler, samt kontorer og arbeidsplasser som kun er ment å være tilgjengelige for relevante ansatte og tjenesteleverandører, er områder som ikke er offentlig tilgjengelige. Offentlig tilgjengelige områder bør ikke omfatte fengsler eller grensekontroll. Enkelte andre rom kan bestå av både offentlig tilgjengelige og ikke-offentlig tilgjengelige rom, for eksempel gangen i en privat boligbygning som er nødvendig for å komme til et legekontor eller en flyplass. Nettbaserte rom er ikke omfattet, ettersom de ikke er fysiske rom. Hvorvidt et gitt rom er tilgjengelig for allmennheten, bør imidlertid avgjøres fra sak til sak, med hensyn til de spesifikke forholdene i den aktuelle situasjonen.

(20) For å oppnå størst mulig nytte av aI-systemer, samtidig som grunnleggende rettigheter, helse og sikkerhet beskyttes, og for å muliggjøre demokratisk kontroll, bør aI-kompetanse utstyre leverandører, brukere og berørte personer med de nødvendige begrepene for å kunne ta informerte beslutninger om aI-systemer. Disse begrepene kan variere med hensyn til den relevante konteksten og kan omfatte forståelse av riktig anvendelse av tekniske elementer i AI-SYSTEMETS utviklingsfase, tiltakene som skal anvendes under bruken, egnede måter å tolke aI-systemets resultater på, og, når det gjelder berørte personer, den kunnskapen som er nødvendig for å forstå hvordan beslutninger som tas ved hjelp av AI, vil påvirke dem. I forbindelse med anvendelsen av denne forordningen bør kunnskap om AI gi alle relevante aktører i aI-verdikjeden den innsikten som kreves for å sikre riktig etterlevelse og korrekt håndheving. Videre vil en bred gjennomføring av tiltak for å øke kunnskapen om kunstig intelligens og innføring av egnede oppfølgingstiltak kunne bidra til å forbedre arbeidsvilkårene og til syvende og sist støtte konsolideringen og innovasjonsutviklingen av pålitelig kunstig INTELLIGENS i Unionen. Det europeiske styret for kunstig intelligens ("styret") bør støtte Kommisjonen i arbeidet med å fremme verktøy for aI-kompetanse, offentlig bevissthet og forståelse av fordelene, risikoene, sikkerhetstiltakene, rettighetene og pliktene knyttet til bruken av aI-systemer. I samarbeid med de relevante interessentene bør Kommisjonen og medlemsstatene legge til rette for at det utarbeides frivillige atferdskodekser for å fremme kunnskap om kunstig intelligens blant personer som arbeider med utvikling, drift og bruk av kunstig intelligens.

(21) For å sikre like vilkår og et effektivt vern av enkeltpersoners rettigheter og friheter i hele Unionen bør reglene som fastsettes ved denne forordning, få anvendelse på tilbydere AV KI-systemer på en ikke-diskriminerende måte, uavhengig av om de er etablert i Unionen eller i en tredjestat, og på brukere AV KI-systemer som er etablert i Unionen.

(22) I lys av deres digitale natur bør visse aI-systemer omfattes av denne forordning selv om de ikke bringes i omsetning, tas i bruk eller brukes i Unionen. Dette er for eksempel tilfelle når en operatør som er etablert i Unionen, inngår avtale om visse tjenester med en operatør som er etablert i en tredjestat, i forbindelse med en aktivitet som skal utføres av et aI-system som kan betegnes som høyrisikosystem. Under slike omstendigheter kan KI-systemet som operatøren bruker i en tredjestat, behandle opplysninger som er lovlig innsamlet i og overført fra Unionen, og gi den kontraherende operatøren I Unionen resultatet av denne behandlingen fra KI-systemet, uten at KI-SYSTEMET bringes i omsetning, tas i bruk eller brukes i Unionen. For å hindre omgåelse av denne forordning og for å sikre et effektivt vern AV fysiske personer som befinner seg i Unionen, bør denne forordning også få anvendelse på tilbydere og ibruktakere AV KI-systemer som er etablert i en , I den utstrekning det som produseres av disse systemene, er beregnet på Å bli brukt i Unionen. For å ta til eksisterende ordninger og særlige behov for framtidig samarbeid med utenlandske partnere som det utveksles informasjon og bevismateriale med, bør denne forordning likevel ikke få anvendelse på offentlige myndigheter i en tredjestat og internasjonale organisasjoner når de opptrer innenfor rammen av samarbeidsavtaler eller internasjonale avtaler som er inngått på unionsplan eller nasjonalt plan for rettshåndhevelse og rettslig samarbeid med Unionen eller medlemsstatene, forutsatt at den relevante tredjestaten eller internasjonale organisasjonen gir tilstrekkelige garantier med hensyn til vern av fysiske personers grunnleggende rettigheter og friheter. Der det er relevant, kan dette omfatte virksomheten til enheter som er betrodd av tredjestatene å utføre bestemte oppgaver til støtte for slikt rettshåndhevelsessamarbeid og rettslig samarbeid. Slike rammer for samarbeid eller avtaler er etablert bilateralt mellom medlemsstatene og tredjestater eller mellom Den europeiske union, Europol og andre EU-byråer og tredjestater og internasjonale organisasjoner. Myndighetene med ansvar for tilsyn med de rettshåndhevende og rettslige myndigheter i henhold til denne forordning bør vurdere om disse rammene for samarbeid eller internasjonale avtaler omfatter tilstrekkelige garantier med hensyn til vern av enkeltpersoners grunnleggende rettigheter og friheter. Mottakende nasjonal

myndigheter og Unionens institusjoner, organer, kontorer og byråer som benytter seg av slike resultater i Unionen, fortsatt er ansvarlige for å sikre at bruken av dem er i samsvar med unionsretten. Når disse internasjonale avtalene revideres eller nye inngås i fremtiden, bør avtalepartene gjøre sitt ytterste for å bringe disse avtalene i samsvar med kravene i denne forordning.

(23) Denne forordning bør også få anvendelse på Unionens institusjoner, organer, kontorer og byråer når de opptrer som leverandør eller distributør AV ET KI-system.

(24) DERSOM OG I DEN UTSTREKNING AI-systemer bringes i omsetning, tas i bruk eller brukes med eller uten endringer av slike systemer for militære formål, forsvarsformål eller nasjonale sikkerhetsformål, bør de unntas fra denne forordnings virkeområde, uavhengig av hvilken type enhet som utøver denne virksomheten, for eksempel om det er en offentlig eller privat enhet. Når det gjelder militære formål og forsvarsformål, er et slikt unntak begrunnet både i artikkel 4 nr. 2 i TEU og i særtrekkene ved medlemsstatenes og Unionens felles forsvarspolitikk som omfattes av kapittel 2 i avdeling V i TEU, og som er underlagt folkeretten, som derfor er den mer egnede rettslige rammen for regulering av KI-SYSTEMER i forbindelse med bruk av dødelig makt og andre KI-systemer i forbindelse med militær virksomhet og forsvarsvirksomhet. Når det gjelder nasjonale sikkerhetsformål, er unntaket begrunnet både med det faktum at nasjonal sikkerhet fortsatt er medlemsstatenes eneansvar i samsvar med artikkel 4 nr. 2 TEU, og med den spesifikke karakteren og de operative behovene til nasjonale sikkerhetsaktiviteter og de spesifikke nasjonale reglene som gjelder for disse aktivitetene. Dersom ET AI-system som er utviklet, markedsført, tatt i bruk eller brukt til militære formål, forsvarsformål eller nasjonale sikkerhetsformål, likevel brukes utenfor disse formålene, midlertidig eller permanent, til andre formål, f.eks. sivile eller humanitære formål, rettshåndhevelse eller offentlig sikkerhet, vil et slikt system falle inn under denne forordnings virkeområde. I så fall bør enheten som bruker AI-SYSTEMET til andre formål enn militære formål, forsvarsformål eller nasjonale sikkerhetsformål, sikre at AI-SYSTEMET er i samsvar med denne forordning, med mindre systemet allerede er i samsvar med denne forordning. aI-systemer som bringes I omsetning eller tas i bruk for et unntatt formål, nemlig militære formål, forsvarsformål eller nasjonale sikkerhetsformål, og ett eller flere ikke-unntatte formål, f.eks. sivile formål eller rettshåndhevelse, faller inn under denne forordnings virkeområde, og tilbydere av disse systemene bør sikre at de er I samsvar med denne forordning. I slike tilfeller bør det faktum at et KI-system kan falle inn under denne forordnings virkeområde, ikke påvirke muligheten for enheter som utøver nasjonale sikkerhets-, forsvars- og militære aktiviteter, uavhengig av hvilken type enhet som disse aktivitetene, til å bruke KI-systemer for nasjonale sikkerhets-, militær- og forsvarsformål, hvis bruk er utelukket fra denne forordnings virkeområde. et KI-system som bringes i omsetning for sivile formål eller rettshåndhevelsesformål, og som med eller uten endringer brukes til militære formål, forsvarsformål eller nasjonale sikkerhetsformål, bør ikke falle under denne forordnings virkeområde, uavhengig av hvilken type enhet som utøver disse aktivitetene.

(25) Denne forordning bør støtte innovasjon, respektere vitenskapens frihet og ikke undergrave forsknings- og utviklingsvirksomhet. Det er derfor nødvendig å utelukke KI-systemer og -modeller som er spesielt utviklet og tatt i bruk utelukkende med henblikk på vitenskapelig forskning og utvikling, fra forordningens virkeområde. Videre er det nødvendig å sikre at denne forordning ikke på annen måte påvirker vitenskapelig forsknings- og utviklingsvirksomhet på KI-systemer eller -modeller før de bringes I omsetning eller tas i bruk. Når det gjelder produktorientert forskning, prøving og utvikling av KI-systemer eller -modeller, bør bestemmelsene i denne forordning heller ikke få anvendelse før disse systemene og modellene tas i bruk eller bringes i omsetning. Dette unntaket berører ikke plikten til å overholde denne forordning dersom et aI-system som omfattes av denne forordnings virkeområde, bringes i omsetning eller tas i bruk som et resultat av slik forsknings- og utviklingsvirksomhet, og anvendelsen av bestemmelser om aI-regulatoriske sandkasser og utprøving under reelle forhold. Uten at det berører utelukkelsen av KI-systemer som er spesielt utviklet og tatt i bruk utelukkende med henblikk på vitenskapelig forskning og utvikling, bør dessuten ethvert annet KI-system som kan brukes til å utføre forsknings- og utviklingsvirksomhet, fortsatt være underlagt bestemmelsene i denne forordning. Under alle omstendigheter bør all forsknings- og utviklingsvirksomhet utføres i samsvar med anerkjente etiske og faglige standarder for vitenskapelig forskning og bør gjennomføres i samsvar med gjeldende unionsrett.

(26) For å kunne innføre proporsjonalt og effektivt sett med bindende regler for AI-SYSTEMER, bør man følge en klart definert risikobasert tilnærming. Denne tilnærmingen bør skreddersy typen og innholdet i slike regler til intensiteten og omfanget av de risikoene som aI-systemene kan generere. Det er derfor nødvendig å forby visse uakseptable aI-praksiser, å fastsette krav til AI-SYSTEMER med høy risiko og forpliktelser for de relevante operatørene, og å fastsette forpliktelser om åpenhet for visse aI-systemer.

(27) Selv om den risikobaserte tilnærmingen er grunnlaget for et proporsjonalt og effektivt sett med bindende regler, er det viktig å minne om de etiske retningslinjene for pålitelig AI fra 2019, som ble utviklet av den uavhengige HLEG-en for pålitelig AI som ble oppnevnt av Kommisjonen. I disse retningslinjene utviklet HLEG syv ikke-bindende etiske prinsipper for KI, som skal bidra til å sikre at KI er troverdig og etisk forsvarlig. De syv prinsippene omfatter menneskelig medvirkning og tilsyn, teknisk robusthet og sikkerhet, personvern og datastyring, åpenhet, mangfold, ikke-diskriminering og rettferdighet, samfunnsmessig og miljømessig velferd samt ansvarlighet. Uten at det berører de rettslig bindende kravene i denne forordningen og annen gjeldende unionsrett, bidrar disse retningslinjene til utformingen av sammenhengende, pålitelig og menneskesentrert KI, i tråd med charteret og de verdiene som unionen bygger på. i henhold til retningslinjene fra HLEG for KI betyr menneskelig medvirkning og tilsyn at KI-systemer utvikles og brukes som et verktøy som tjener mennesker, respekterer menneskelig verdighet og personlig autonomi, og som fungerer på en måte som kan kontrolleres og overvåkes av mennesker på en hensiktsmessig måte. Teknisk robusthet og sikkerhet betyr at aI-systemer utvikles og brukes på en måte som gjør dem robuste i tilfelle problemer og motstandsdyktige mot forsøk på å endre bruken eller ytelsen til aI-systemet, slik at tredjeparter kan bruke det på ulovlig vis, og slik at utilsiktet skade minimeres. Personvern og datastyring innebærer at AI-SYSTEMENE utvikles og brukes i samsvar med personvernreglene, samtidig som de behandler data som oppfyller høye standarder for kvalitet og integritet. Åpenhet betyr at aI-systemer utvikles og brukes på en måte som gjør det mulig å spore og forklare dem, samtidig som mennesker gjøres oppmerksomme på at de kommuniserer eller samhandler med et aI-system, og brukere informeres om aI-systemets muligheter og begrensninger, og berørte personer informeres om sine rettigheter. Mangfold, ikke-diskriminering og rettferdighet betyr at AI-SYSTEMER utvikles og brukes på en måte som inkluderer ulike aktører og fremmer lik tilgang, likestilling mellom kjønnene og kulturelt mangfold, samtidig som man unngår diskriminerende virkninger og urettferdige fordommer som er forbudt i henhold til unionsretten eller nasjonal lovgivning. Sosial og miljømessig velferd betyr AT KI-systemer utvikles og brukes PÅ en bærekraftig og miljøvennlig måte og på en måte som kommer alle mennesker til gode, samtidig som de langsiktige konsekvensene for individet, samfunnet og demokratiet overvåkes og vurderes. Disse prinsippene bør om mulig omsettes i utformingen og bruken av KI-modeller. De bør under alle omstendigheter tjene som grunnlag for utarbeidelsen av etiske retningslinjer i henhold til denne forordningen. Alle interessenter, herunder næringslivet, akademia, det sivile samfunn og standardiseringsorganisasjoner, oppfordres til å ta hensyn til de etiske prinsippene når det er hensiktsmessig for utviklingen av frivillig beste praksis og standarder.

(28) ved siden av de mange nyttige bruksområdene FOR AI, kan det også misbrukes og gi nye og kraftige verktøy for manipulerende, utnyttende og sosial kontrollpraksis. Slik praksis er særlig skadelig og krenkende og bør forbys fordi den er i strid med Unionens verdier om respekt for menneskeverd, frihet, likhet, demokrati og rettsstatsprinsipper og de grunnleggende rettighetene som er nedfelt i pakten, herunder retten til ikke-diskriminering, til databeskyttelse og til privatlivets fred og barns rettigheter.

(29) AI-AKTIVERTE manipulative teknikker kan brukes til å overtale personer til å engasjere seg i uønsket atferd, eller til å lure dem ved å dytte dem til å ta beslutninger på en måte som undergraver og svekker deres autonomi, beslutningstaking og frie valg. Markedsføring, ibruktaking eller bruk av visse KI-systemer som har til formål eller virkning å vesentlig forvrenge menneskers atferd, slik at det er sannsynlig at det vil oppstå betydelige skader, særlig med tilstrekkelig store negative konsekvenser for fysisk eller psykisk helse eller økonomiske interesser, er særlig farlig og bør derfor forbys. Slike AI-systemer benytter subliminale komponenter som lyd-, bilde- eller videostimuli som personer ikke kan oppfatte, ettersom disse stimuliene er utenfor menneskets persepsjon, eller andre manipulerende eller villedende teknikker som undergraver eller svekker personers autonomi, beslutningstaking eller frie valg på måter som gjør at personer ikke er bevisst disse teknikkene, eller, dersom de er klar over dem, likevel kan bli lurt eller ikke er i stand til å kontrollere eller motstå dem. Dette kan for eksempel gjøres lettere ved hjelp av maskin-hjerne-grensesnitt eller virtuell virkelighet, ettersom de muliggjør en høyere grad av kontroll over hvilke stimuli som presenteres for personer, i den grad kan forvrenge atferden deres på en vesentlig skadelig måte. I tillegg kan KI-systemer også på andre måter utnytte sårbarheten til en person eller en bestemt gruppe personer på grunn av alder, nedsatt funksjonsevne i henhold til Europaparlamentets og Rådets direktiv (EU) 2019/882 ((16)), eller en bestemt sosial eller økonomisk situasjon som sannsynligvis vil gjøre disse personene mer sårbare for utnyttelse, f.eks. personer som lever i ekstrem fattigdom, eller etniske eller religiøse minoriteter. Slike AI-systemer kan bringes I , tas i bruk eller brukes det formål eller den virkning å vesentlig forvrenge atferden til en person og på en måte som forårsaker eller med rimelig sannsynlighet vil forårsake betydelig skade på denne eller en annen person eller grupper av , herunder skader som kan akkumuleres over tid, og som derfor bør forbys. Det er ikke sikkert at det er mulig å anta at det foreligger en

(16) Europaparlaments- og rådsdirektiv (EU) 2019/882 av 17. april 2019 om tilgjengelighetskrav for produkter og tjenester (EUT L 151 av 7.6.2019, s. 70).

intensjon om å forvrenge atferd der forvrengningen skyldes faktorer utenfor aI-systemet som ligger utenfor tilbyderens eller utbyggerens kontroll, det vil si faktorer som kanskje ikke med rimelighet kan forutses og som det derfor ikke er mulig for tilbyderen eller utbyggeren av aI-systemet å redusere. Det er uansett ikke nødvendig at tilbyderen eller utrulleren har til hensikt å forårsake betydelig skade, forutsatt at slik skade skyldes manipulerende eller utnyttende aI-praksiser. Forbudene mot slik aI-praksis utfyller -bestemmelsene i europaparlaments- og rådsdirektiv 2005/29/EF ([17])særlig er urimelig handelspraksis som fører til økonomisk eller finansiell skade for forbrukere, forbudt under alle omstendigheter, uavhengig av om den ER innført gjennom aI-systemer eller på annen måte. Forbudene mot manipulerende og utnyttende praksis i denne forordning bør ikke berøre lovlig praksis i forbindelse med medisinsk behandling, f.eks. psykologisk behandling av en psykisk sykdom eller fysisk rehabilitering, når denne praksisen utføres i samsvar med gjeldende lovgivning og medisinske standarder, f.eks. med uttrykkelig samtykke enkeltpersoner eller deres rettslige representanter. I tillegg bør vanlig og legitim handelspraksis, for eksempel på reklameområdet, som er i samsvar med gjeldende lov, ikke i seg selv anses som skadelig manipulerende INFORMASJONSINNHENTENDE praksis.

(30) Biometriske kategoriseringssystemer som er basert på fysiske personers biometriske opplysninger, f.eksen enkeltpersons ansikt eller fingeravtrykk, for å utlede eller slutte seg til en enkeltpersons politiske oppfatning, fagforeningsmedlemskap, religiøse eller filosofiske overbevisning, rase, kjønnsliv eller seksuelle orientering, bør forbys. Forbudet bør ikke omfatte lovlig merking, filtrering eller kategorisering av biometriske datasett som er innhentet i samsvar med unionsretten eller nasjonal rett, i henhold til biometriske data, for eksempel sortering av bilder etter hårfarge eller øyenfarge, som for eksempel kan brukes i forbindelse med rettshåndhevelse.

(31) AI systemer som gir sosiale poeng til fysiske personer av offentlige eller private aktører, kan føre til diskriminerende resultater og utestenging av visse grupper. De kan være i strid med retten verdighet og ikke-diskriminering og med verdiene likhet og rettferdighet. Slike aI-systemer evaluerer eller klassifiserer fysiske personer eller grupper av fysiske personer på grunnlag av flere datapunkter knyttet til deres sosiale atferd i flere sammenhenger eller kjente, antatte eller forventede personlige eller personlighetsmessige egenskaper over bestemte tidsperioder. Den sosiale poengsummen som oppnås fra slike aI-systemer, kan føre til at fysiske personer eller hele grupper av slike personer behandles ufordelaktig eller ugunstig i sosiale sammenhenger som ikke har sammenheng med den sammenhengen opplysningene opprinnelig ble generert eller innsamlet i, eller til en ufordelaktig behandling som ikke står i forhold til eller er uberettiget i forhold til alvorlighetsgraden av deres sosiale atferd. aI-systemer som innebærer en slik uakseptabel poengsettingspraksis og fører til slike ufordelaktige eller ugunstige resultater, bør derfor forbys. Dette forbudet bør ikke berøre lovlig evalueringspraksis for fysiske personer som utføres for et bestemt formål i samsvar med unionsretten og nasjonal rett.

(32) Bruk av KI-systemer for "sanntids" biometrisk fjernidentifikasjon av fysiske personer på offentlig tilgjengelige steder i rettshåndhevelsesøyemed er særlig inngripende i de berørte personenes rettigheter og friheter, i den grad det kan påvirke privatlivet til en stor del av befolkningen, fremkalle en følelse av konstant overvåking og indirekte motvirke utøvelsen av forsamlingsfriheten og andre grunnleggende rettigheter. Tekniske unøyaktigheter I AI-systemer beregnet for biometrisk identifikasjon av fysiske personer PÅ avstand kan føre til skjeve resultater og ha diskriminerende virkninger. Slike mulige skjeve resultater og diskriminerende virkninger er særlig relevante med hensyn til alder, etnisitet, rase, kjønn eller funksjonshemninger. I tillegg medfører den umiddelbare virkningen og de begrensede mulighetene for ytterligere kontroller eller korrigeringer i forbindelse med bruk av slike systemer som opererer i sanntid, økt risiko for rettighetene og frihetene til de berørte personene i forbindelse med, eller påvirket av, rettshåndhevelsesaktiviteter.

(33) Bruk av disse systemene i rettshåndhevelsesøyemed bør derfor forbys, unntatt i uttømmende opplistede og snevert definerte situasjoner der bruken er strengt nødvendig for å oppnå et vesentlig samfunnshensyn, og der betydningen av dette hensynet veier tyngre enn risikoen. Disse situasjonene omfatter ettersøking av visse ofre for kriminalitet, herunder savnede personer, visse trusler mot fysiske personers liv eller fysiske sikkerhet eller mot et terrorangrep, og lokalisering eller identifisering av gjerningsmenn eller mistenkte for straffbare handlinger som er oppført i et vedlegg til denne forordning, dersom disse straffbare handlingene kan straffes med frihetsstraff eller varetektsfengsling i den berørte medlemsstaten.

(17) Europaparlaments- og rådsdirektiv 2005/29/EF av 11. mai 2005 om foretaks urimelige handelspraksis overfor forbrukere i det indre marked og om endring av RÅDSDIREKTIV 84/450/EØF, europaparlaments- og rådsdirektiv 97/7/EF, 98/27/EF og 2002/65/EF og og rådsforordning (EF) nr. 2006/2004 ("direktivet om urimelig handelspraksis") (EUT L 149 av 11.6.2005, s. 22).

for en maksimumsperiode på minst fire år, og slik de er definert i den aktuelle medlemsstatens lovgivning. En slik terskel for frihetsstraff eller frihetsberøvelse i samsvar med nasjonal lovgivning bidrar til å sikre at lovbruddet bør være alvorlig nok til å kunne rettferdiggjøre bruk av systemer for biometrisk fjernidentifikasjon i sanntid. Videre er listen over straffbare handlinger i vedlegget til denne forordning basert på de 32 straffbare handlingene som er oppført i Rådets rammeavgjørelse 2002/584/JHA ([18]), idet det tas hensyn til at noen av disse handlingene i praksis sannsynligvis vil være mer relevante enn andre, i og med at bruk av biometrisk fjernidentifikasjon i "sanntid" kan forutsigbart være nødvendig og forholdsmessig i svært varierende grad i praksis å lokalisere eller identifisere en gjerningsperson eller mistenkt for de ulike opplistede straffbare handlinger, og idet det tas hensyn til de sannsynlige forskjellene i skadevirkningens eller de mulige negative konsekvensers alvor, sannsynlighet og omfang. En overhengende trussel mot fysiske personers liv eller fysiske sikkerhet kan også følge av en alvorlig forstyrrelse av kritisk infrastruktur, som definert i artikkel 2 nr. 4 i europaparlaments- og rådsdirektiv (EU) 2022/2557 [19], dersom forstyrrelsen eller ødeleggelsen av slik kritisk infrastruktur vil føre til en overhengende trussel mot en persons liv eller fysiske sikkerhet, herunder gjennom alvorlig skade på forsyningen av grunnleggende forsyninger til befolkningen eller på utøvelsen av statens kjernefunksjon. I tillegg bør denne forordning bevare muligheten for rettshåndhevelses-, grensekontroll-, innvandrings- eller asylmyndigheter til å utføre identitetskontroller i den berørte personens nærvær i samsvar med vilkårene som er fastsatt i unionsretten og nasjonal rett for slike kontroller. Navnlig bør rettshåndhevelses-, grensekontroll-, innvandrings- eller asylmyndigheter bruke informasjonssystemer, i samsvar med unionsretten eller nasjonal rett, til å identifisere personer som under en identitetskontroll enten nekter å la seg identifisere eller ikke er i stand til å oppgi eller bevise sin identitet, uten at det i henhold til denne forordning kreves at det innhentes forhåndstillatelse. Dette kan for eksempel være en person som er innblandet i en forbrytelse, som er uvillig eller ute av stand til å oppgi sin identitet til rettshåndhevende myndigheter på grunn av en ulykke eller en medisinsk tilstand.

(34) For å sikre at disse systemene brukes på en ansvarlig og forholdsmessig måte, er det også viktig å fastslå at det i hver av disse uttømmende opplistede og snevert definerte situasjonene bør tas hensyn til visse elementer, særlig med hensyn til arten av situasjonen som gir opphav til anmodningen, og konsekvensene av bruken alle berørte personers rettigheter og friheter og de garantier og vilkår som er fastsatt for bruken. I tillegg bør bruken av "sanntids" fjernstyrte biometriske identifikasjonssystemer i offentlig tilgjengelige områder i rettshåndhevelsesøyemed bare brukes for å bekrefte identiteten til den spesifikt målrettede personen og bør begrenses til det som er strengt nødvendig med hensyn til tidsperioden, samt det geografiske og personlige omfanget, særlig med hensyn til bevis eller indikasjoner på truslene, ofrene eller gjerningsmannen. Bruk av systemet for fjernstyrt biometrisk identifikasjon i sanntid på offentlig tilgjengelige steder bør bare tillates dersom den relevante rettshåndhevelsesmyndigheten har gjennomført en konsekvensanalyse av de grunnleggende rettighetene og, med mindre annet er fastsatt i denne forordning, har registrert systemet i databasen som fastsatt i denne forordning. Referansedatabasen over personer bør være egnet for hvert brukstilfelle i hver av situasjonene nevnt ovenfor.

(35) Enhver bruk av et system for fjernstyrt biometrisk identifikasjon i "sanntid" på offentlig tilgjengelige steder med henblikk på rettshåndhevelse bør være underlagt en uttrykkelig og spesifikk tillatelse fra en rettslig myndighet eller fra en uavhengig administrativ myndighet i en medlemsstat, hvis avgjørelse er bindende. En slik tillatelse bør i prinsippet innhentes før KI-systemet tas i bruk med sikte på å identifisere en eller flere personer. Unntak fra denne regelen bør tillates i behørig begrunnede hastesituasjoner, dvs. i situasjoner der behovet for å bruke de berørte systemene er av en slik art at det er faktisk og objektivt umulig å innhente en tillatelse før bruken AV aI-systemet påbegynnes. I slike hastesituasjoner bruken AV aI-systemet begrenses det absolutt nødvendige minimum og være underlagt egnede garantier og vilkår, som fastsatt i nasjonal rett og spesifisert i forbindelse med hver enkelt hastesak av den rettshåndhevende myndighet selv. I tillegg bør rettshåndhevelsesmyndigheten i slike situasjoner anmode om slik tillatelse og samtidig til at den ikke har kunnet anmode om den tidligere, uten ugrunnet opphold og senest innen 24 timer. Dersom en slik tillatelse avslås, bør bruken av biometriske sanntidsidentifikasjonssystemer knyttet til denne tillatelsen opphøre med umiddelbar virkning, og alle opplysninger knyttet til slik bruk bør kasseres og slettes. Slike opplysninger omfatter

(18) Rådets rammeavgjørelse 2002/584/JHA av 13. juni 2002 om den europeiske arrestordren og overleveringsprosedyrene mellom medlemsstatene (EFT L 190 av 18.7.2002, s. 1).

(19) Europaparlaments- og rådsdirektiv (EU) 2022/2557 av 14. desember 2022 om kritiske enheters motstandsdyktighet og om oppheving av rådsdirektiv 2008/114/EF (EUT L 333 av 27.12.2022, s. 164).

inndata som er direkte innhentet AV ET AI-system i løpet av bruken av et slikt system, samt resultater og utdata fra bruken knyttet til denne . Det bør ikke omfatte inndata som er lovlig innhentet i samsvar med annen unionsrett eller nasjonal rett. Under enhver omstendighet bør det ikke treffes noen beslutning som har negative rettsvirkninger for en person, utelukkende på grunnlag av resultatene fra det biometriske fjernidentifikasjonssystemet.

(36) For at de skal kunne utføre sine oppgaver i samsvar med kravene fastsatt i denne forordning og i nasjonale regler, bør den relevante markedstilsynsmyndigheten og den nasjonale personvernmyndigheten underrettes om hver bruk av systemet for biometrisk identifikasjon i sanntid. Markedstilsynsmyndighetene og de nasjonale personvernmyndighetene som er blitt underrettet, bør sende Kommisjonen en årlig rapport om bruken av biometriske sanntidsidentifikasjonssystemer.

(37) Videre er det hensiktsmessig å fastsette, innenfor den uttømmende rammen som er fastsatt i denne forordning, at slik bruk på en medlemsstats territorium i samsvar med denne forordning bare bør være mulig dersom og i den utstrekning den berørte medlemsstaten har besluttet å gi uttrykkelig mulighet til å tillate slik bruk i sine nærmere bestemmelser i nasjonal rett. Følgelig står medlemsstatene i henhold til denne forordning fritt til ikke å fastsette en slik mulighet i det hele tatt eller til bare å fastsette en slik mulighet med hensyn til noen av de formål som kan begrunne tillatt bruk, og som er angitt i denne forordning. Slike nasjonale regler bør meldes til Kommisjonen innen 30 dager etter at de er vedtatt.

(38) Bruken AV KI-systemer for fjernstyrt biometrisk sanntidsidentifikasjon av fysiske personer i offentlig tilgjengelige områder med henblikk på rettshåndhevelse innebærer nødvendigvis behandling av biometriske opplysninger. Reglene i denne forordning som, med visse unntak, forbyr slik bruk, og som er basert på artikkel 16 i TEUV, bør få anvendelse som *lex specialis* med hensyn til reglene om behandling av biometriske opplysninger i artikkel 10 i direktiv (EU) 2016/680, og dermed regulere slik bruk og behandlingen av de berørte biometriske opplysningene på en uttømmende måte. Derfor bør slik bruk og behandling bare være mulig i den utstrekning det er forenlig med rammen fastsatt i denne forordning, uten at det utenfor denne rammen er rom at vedkommende myndigheter, når de opptrer med henblikk på rettshåndheving, kan bruke slike systemer og behandle slike opplysninger i forbindelse med dette på de grunnlag som er oppført i artikkel 10 i direktiv (EU) 2016/680. I denne sammenheng er denne forordning ikke ment å gi rettslig grunnlag for behandling av personopplysninger i henhold til artikkel 8 i direktiv (EU) 2016/680. Bruk av systemer for fjernstyrt biometrisk identifikasjon i sanntid på offentlig tilgjengelige steder for andre formål enn rettshåndhevelse, herunder av vedkommende myndigheter, bør imidlertid ikke omfattes av de særlige rammene for slik bruk rettshåndhevelsesformål som er fastsatt i denne forordning. Slik bruk til andre formål enn rettshåndhevelse bør derfor ikke være underlagt kravet om tillatelse i henhold til denne forordning og de gjeldende detaljerte reglene i nasjonal lovgivning som kan gi denne tillatelsen virkning.

(39) all behandling av biometriske opplysninger og andre personopplysninger som er involvert i bruken AV KI-systemer for biometrisk identifikasjon, bortsett fra i forbindelse med bruk av fjernstyrte biometriske identifikasjonssystemer i sanntid på offentlig tilgjengelige steder med henblikk på rettshåndhevelse som regulert i denne forordning, bør fortsatt oppfylle alle krav som følger av artikkel 10 i direktiv (EU) 2016/680. For andre formål enn rettshåndhevelse forbyr artikkel 9 nr. 1 i forordning (EU) 2016/679 og artikkel 10 nr. 1 i forordning (EU) 2018/1725 behandling av biometriske opplysninger med forbehold om begrensede unntak som fastsatt i disse artiklene. Ved anvendelsen av artikkel 9 nr. 1 i forordning (EU) 2016/679 har bruken av biometrisk fjernidentifikasjon til andre formål enn rettshåndhevelse allerede vært gjenstand for forbudsvedtak av nasjonale personvernmyndigheter.

(40) I samsvar med artikkel 6a i protokoll nr. 21 om Det forente kongerikes og Irlands stilling med hensyn til området med frihet, sikkerhet og rettferdighet, som er knyttet som vedlegg til TEU og til TEUV, er Irland ikke bundet av reglene fastsatt i artikkel 5 nr. 1 første ledd bokstav g), I den utstrekning den får anvendelse på bruken av biometriske kategoriseringssystemer for virksomhet på området politisamarbeid og strafferettslig samarbeid, artikkel 5 nr. 1 første ledd bokstav d), i den utstrekning den får anvendelse på bruken AV AI-systemer som omfattes av nevnte bestemmelse, artikkel 5 nr. 1 første ledd bokstav h), artikkel 5 nr. 2-6 og ARTIKKEL 26 nr. 10 i denne forordning vedtatt på grunnlag av artikkel 16 i TEUV, som gjelder medlemsstatenes behandling av personopplysninger når de utøver virksomhet som omfattes av virkeområdet for tredje del avdeling V kapittel 4 eller kapittel 5 i TEUV, der Irland ikke er bundet av reglene for de former for strafferettslig samarbeid eller politisamarbeid som krever overholdelse av bestemmelsene fastsatt på grunnlag av artikkel 16 i TEUV.

(41) I samsvar med artikkel 2 og 2a i protokoll nr. 22 om Danmarks stilling, som er knyttet til TEU og TEUV, er Danmark ikke bundet av reglene fastsatt i artikkel 5 nr. 1 første ledd bokstav g), i den utstrekning den får anvendelse på bruk av biometriske kategoriseringssystemer i med aktiviteter innen politisamarbeid og strafferettslig samarbeid, artikkel 5 nr. 1 første ledd bokstav d), i den utstrekning den får anvendelse på bruk AV AI-systemer som omfattes av nevnte bestemmelse, artikkel 5 nr. 1 første ledd bokstav h), nr. 2 til 6 og artikkel 26 nr. 10 i denne forordning

vedtatt på grunnlag av artikkel 16 i TEUV, eller med forbehold om deres anvendelse, som gjelder medlemsstatenes behandling av personopplysninger når de utøver virksomhet som faller inn under virkeområdet til tredje del avdeling V kapittel 4 eller kapittel 5 i TEUV.

(42) I tråd med uskyldspresumsjonen bør fysiske personer i Unionen alltid bedømmes ut fra sin faktiske atferd. Fysiske personer bør aldri bedømmes ut fra EN FORVENTET atferd utelukkende basert på deres profilering, personlighetstrekk eller kjennetegn, som nasjonalitet, fødested, bosted, antall barn, gjeldsnivå eller biltype, uten at det foreligger en begrunnet mistanke om at vedkommende er involvert i en kriminell aktivitet basert på objektive, verifiserbare fakta og uten menneskelig vurdering av disse. Det bør derfor være forbudt å foreta risikovurderinger av fysiske personer for å vurdere sannsynligheten for at de vil begå lovbrudd, eller for å forutsi forekomsten av en faktisk eller potensiell straffbar handling, utelukkende på grunnlag av profilering av dem eller vurdering av deres personlighetstrekk og egenskaper. Dette forbudet viser uansett ikke til eller berører risikoanalyser som ikke er basert på profilering AV enkeltpersoner eller på enkeltpersoners personlighetstrekk og egenskaper, for eksempel AI-systemer som bruker risikoanalyser for å vurdere sannsynligheten for økonomisk svindel begått av foretak på grunnlag av mistenkelige transaksjoner, eller risikoanalyseverktøy for å forutsi sannsynligheten for tollmyndighetenes lokalisering av narkotika eller ulovlige varer, for eksempel på grunnlag av kjente smuglerruter.

(43) Det bør forbys å markedsføre, ta i bruk eller bruke KI-systemer som oppretter eller utvider ansiktsgjenkjenningsdatabaser ved hjelp av målrettet skraping av ansiktsbilder fra internett eller overvåkingsbilder, fordi denne praksisen forsterker følelsen av masseovervåking og kan føre til grove krenkelser av grunnleggende rettigheter, herunder retten til privatliv.

(44) Det er alvorlige bekymringer knyttet til det vitenskapelige grunnlaget for KI-systemer som tar sikte på å identifisere eller utlede følelser, særlig fordi følelsesuttrykk varierer betydelig på tvers av kulturer og situasjoner, og til og med innenfor et enkelt individ. blant de viktigste svakhetene ved slike systemer er den begrensede påliteligheten, mangelen på spesifisitet og den begrensede generaliserbarheten. KI-systemer som identifiserer eller utleder følelser eller intensjoner hos fysiske personer på grunnlag av deres biometriske data, kan derfor føre til diskriminerende resultater og kan gripe i de berørte personenes rettigheter og friheter. Tatt i betraktning den skjeve maktbalansen i forbindelse med arbeid eller utdanning, kombinert med disse systemenes inngripende karakter, kan slike systemer føre til skadelig eller ufordelaktig behandling av visse fysiske personer eller hele grupper av disse. Det bør derfor forbys å bringe I , ta i bruk eller bruke KI-systemer som er beregnet på å brukes til å registrere enkeltpersoners følelsesmessige tilstand i situasjoner knyttet til arbeidsplassen og utdanning. Dette forbudet bør ikke omfatte KI-systemer som bringes i omsetning av rent medisinske eller sikkerhetsmessige grunner, for eksempel systemer beregnet på terapeutisk bruk.

(45) Praksis som er forbudt i henhold til unionsretten, herunder personvernlovgivning, ikke-diskrimineringslovgivning, forbrukervernlovgivning og konkurranselovgivning, bør ikke berøres av denne forordningen.

(46) HØYRISIKO-AI-SYSTEMER bør bare bringes i omsetning på unionsmarkedet, tas i bruk eller brukes dersom de oppfyller visse obligatoriske krav. Disse kravene bør sikre AT høyrisiko-AI-systemer som er tilgjengelige i Unionen, eller hvis resultater på annen måte brukes i Unionen, ikke utgjør en uakseptabel risiko for viktige offentlige interesser i Unionen, slik disse er anerkjent og beskyttet i unionsretten. På grunnlag av det nye lovgivningsrammeverket, som klargjort i Kommisjonens kunngjøring "The "Blue Guide" on the implementation of EU product rules 2022" ([20], er den generelle regelen at mer enn én rettsakt i Unionens harmoniseringslovgivning, som europaparlaments- og rådsforordning (EU) 2017/745 ([21])[22] (EU) 2017/746 eller europaparlaments- og rådsdirektiv 2006/42/EF ([23], kan få anvendelse på ett produkt, siden tilgjengeliggjøring eller ibruktaking kan skje

(20) EUT C 247 av 29.6.2022, s. 1.

(21) Europaparlaments- og rådsforordning (EU) 2017/745 av 5. april 2017 om medisinsk utstyr, om endring av direktiv 2001/83/EF, forordning (EF) nr. 178/2002 og forordning (EF) nr. 1223/2009 og om oppheving av rådsdirektiv 90/385/EØF og 93/42/EØF (EUT L 117 av 5.5.2017, s. 1).

(22) Europaparlaments- og rådsforordning (EU) 2017/746 av 5. april 2017 om medisinsk utstyr til *in* vitro-diagnostikk og om oppheving av direktiv 98/79/EF og kommisjonsbeslutning 2010/227/EU (EUT L 117 av 5.5.2017, s. 176).

(23) Europaparlaments- og rådsdirektiv 2006/42/EF av 17. mai 2006 om maskiner og om endring av direktiv 95/16/EF (EUT L 157 av 9.6.2006, s. 24).

bare finne sted når produktet er i samsvar med all gjeldende harmoniseringslovgivning i Unionen. For å sikre konsekvens og unngå unødvendige administrative byrder eller kostnader bør leverandører av produkt som inneholder ett eller flere høyrisikosystemer, som kravene i denne forordning og i Unionens harmoniseringsregelverk oppført i et vedlegg til denne forordning får anvendelse på, ha fleksibilitet med hensyn til operasjonelle beslutninger om hvordan de på best mulig måte kan sikre at et produkt som inneholder ett eller flere høyrisikosystemer, er i samsvar med alle gjeldende krav i Unionens harmoniseringsregelverk. AI-SYSTEMER som identifiseres som høyrisikosystemer, bør begrenses til dem som har en betydelig skadelig innvirkning på helse, sikkerhet og grunnleggende rettigheter for personer i Unionen, og en slik begrensning bør minimere enhver potensiell begrensning av internasjonal handel.

(47) aI-systemer kan ha en negativ innvirkning på menneskers helse og sikkerhet, særlig når slike systemer fungerer som sikkerhetskomponenter I produkter. I samsvar med målene i Unionens harmoniseringslovgivning om å legge til rette for fri bevegelighet for produkter i det indre marked og sikre at bare sikre og ellers kompatible produkter finner veien til markedet, er det viktig at sikkerhetsrisikoen som kan genereres av et produkt som på grunn av dets digitale komponenter, herunder AI-SYSTEMER, forebygges og reduseres på behørig vis. For eksempel bør stadig mer autonome roboter, enten det dreier seg om produksjon eller personlig assistanse og pleie, være i stand til å operere og utføre sine funksjoner i komplekse miljøer på en sikker måte. I helsesektoren, der liv og helse står på spill, bør stadig mer sofistikerte diagnosesystemer og systemer som støtter menneskelige beslutninger, være pålitelige og nøyaktige.

(48) Omfanget av den negative innvirkningen som aI-systemet har på de grunnleggende rettighetene som er beskyttet av charteret, er av særlig relevans når et AI-SYSTEM klassifiseres som høyrisiko. Disse rettighetene omfatter retten til menneskeverd, respekt privat- og familieliv, beskyttelse av personopplysninger, ytrings- og informasjonsfrihet, forsamlings- og foreningsfrihet, retten til ikke-diskriminering, retten til utdanning, forbrukervern, arbeidstakerrettigheter, rettighetene til personer med nedsatt funksjonsevne, likestilling mellom kjønnene, immaterielle rettigheter, retten til et effektivt rettsmiddel og til en rettferdig rettergang, retten til forsvar og uskyldspresumsjonen samt retten til god forvaltning. I tillegg til disse rettighetene er det viktig å fremheve at barn har spesifikke rettigheter som er nedfelt i artikkel 24 i pakten og i FNs barnekonvensjon, som er videreutviklet i barnekonvensjonens generelle kommentar nr. 25 om det digitale miljøet, og som begge krever at det tas hensyn til barns sårbarhet og at de gis den beskyttelse og omsorg som er nødvendig for deres velferd. Den grunnleggende retten til et høyt miljøvernnivå som er nedfelt i pakten og gjennomført i Unionens politikk, bør også tas I betraktning ved vurderingen av hvor alvorlig skade ET AI-system kan forårsake, blant annet med hensyn til menneskers helse og sikkerhet.

(49) når det gjelder høyrisikosystemer som er sikkerhetskomponenter i produkter eller systemer, eller som selv er produkter eller systemer som faller inn under virkeområdet til europaparlaments- og rådsforordning ([24]EF) nr. 300/2008 , europaparlaments- og rådsforordning (EU) nr. 167/2013 [25])Regulation (EU) No 168/2013 of the European Parliament and of the Council ([26]), directive 2014/90/EU of the European Parliament and of the Council ([27]), directive (EU) 2016/797 of the European Parliament and of the Council ([28]), Regulation (EU) 2018/858 of the European Parliament and of the Council ([29]), Regulation (EU) 2018/1139 of the

(24) Europaparlaments- og rådsforordning (EF) nr. 300/2008 av 11. mars 2008 om felles bestemmelser om sikkerhet innen sivil luftfart og om oppheving av forordning (EF) nr. 2320/2002 (EUT L 97 av 9.4.2008, s. 72).

(25) Europaparlaments- og rådsforordning (EU) nr. 167/2013 av 5. februar 2013 om godkjenning og markedstilsyn av landbruks- og skogbrukskjøretøyer (EUT L 60 av 2.3.2013, s. 1).

(26) Europaparlaments- og rådsforordning (EU) nr. 168/2013 av 15. januar 2013 om godkjenning og markedstilsyn av to- og trehjulede kjøretøyer og firehjulinger (EUT L 60 av 2.3.2013, s. 52).

(27) Europaparlaments- og rådsdirektiv 2014/90/EU av 23. juli 2014 om skipsutstyr og om oppheving av rådsdirektiv 96/98/EF (EUT L 257 av 28.8.2014, s. 146).

(28) Europaparlaments- og rådsdirektiv (EU) 2016/797 av 11. mai 2016 om samtrafikkevnen i jernbanesystemet i Den europeiske union (EUT L 138 av 26.5.2016, s. 44).

(29) Europaparlaments- og rådsforordning (EU) 2018/858 av 30. mai 2018 om godkjenning og markedstilsyn av motorvogner og tilhengere til disse og av systemer, komponenter og separate tekniske enheter beregnet på slike kjøretøyer, om endring av forordning (EF) nr. 715/2007 og (EF) nr. 595/2009 og om oppheving av direktiv 2007/46/EF (EUT L 151 av 14.6.2018, s. 1).

Europaparlamentet og Rådet [30]) og europaparlaments- og rådsforordning (EU) 2019/2144 ([31]), er det hensiktsmessig å endre disse rettsaktene for å sikre at Kommisjonen, på grunnlag av de tekniske og reguleringsmessige særtrekkene ved hver sektor, og uten å gripe inn i eksisterende styrings-, og håndhevingsmekanismer og myndigheter som er etablert der, tar hensyn til de obligatoriske kravene til høyrisikosystemer som ER fastsatt i denne forordning, når den vedtar relevante delegerte rettsakter eller gjennomføringsrettsakter på grunnlag av nevnte rettsakter.

(50) Når det gjelder AI-systemer som er sikkerhetskomponenter i produkter, eller som i seg selv er produkter, som omfattes av virkeområdet for visse unionsharmoniseringsregelverk oppført i et vedlegg til denne forordning, er det hensiktsmessig å klassifisere dem som høyrisikoprodukter i henhold til denne forordning dersom det berørte produktet gjennomgår framgangsmåten for samsvarsvurdering med et tredjepartsorgan for samsvarsvurdering i henhold til det relevante unionsharmoniseringsregelverket. Slike produkter er særlig maskiner, leketøy, heiser, utstyr og sikringssystemer beregnet på bruk i eksplosjonsfarlig atmosfære, radioutstyr, trykkpåkjent utstyr, utstyr til fritidsfartøyer, taubaneanlegg, apparater som bruker gassformig brensel, medisinsk utstyr, medisinsk utstyr til *in* vitro-diagnostikk, bil- og luftfart.

(51) Klassifiseringen av et KI-system som høyrisiko i henhold til denne forordning bør ikke nødvendigvis bety at produktet som har som sikkerhetskomponent, eller selve KI-systemet som produkt, anses som høyrisiko i henhold til kriteriene som er fastsatt i den relevante harmoniseringslovgivningen i Unionen som får anvendelse på produktet. Dette gjelder særlig forordning (EU) 2017/745 og (EU) 2017/746, der det er fastsatt en tredjeparts samsvarsvurdering for produkter med middels risiko og høy risiko.

(52) Når det gjelder frittstående AI-SYSTEMER, dvs. andre høyrisikosystemer enn dem som er sikkerhetskomponenter i produkter, eller som selv er produkter, er det hensiktsmessig å klassifisere dem som høyrisikosystemer dersom de, I lys sitt tiltenkte formål, utgjør en høy risiko for skade på menneskers helse og sikkerhet eller grunnleggende rettigheter, idet det tas hensyn til både alvorlighetsgraden av den mulige skaden og sannsynligheten for at den skal inntreffe, og dersom de brukes på en rekke spesifikt forhåndsdefinerte områder som er angitt i denne forordning. Identifikasjonen av disse systemene er basert på den samme metodikken og de samme kriteriene som er planlagt også for eventuelle fremtidige endringer av listen over høyrisikosystemer for KUNSTIG INTELLIGENS som Kommisjonen bør gis myndighet til å vedta ved hjelp av delegerte rettsakter, for å ta hensyn til DEN raske teknologiske utviklingen og de potensielle endringene i bruken AV systemer FOR KUNSTIG INTELLIGENS.

(53) Det er også viktig å presisere at det kan finnes særlige tilfeller der KI-systemer som er nevnt i forhåndsdefinerte områder angitt i denne forordning, ikke fører til en betydelig risiko for skade på de rettslige interessene som er beskyttet under disse områdene, fordi de ikke påvirker beslutningsprosessen i vesentlig grad eller ikke skader disse interessene I vesentlig grad. I denne forordning bør et KI-system som ikke påvirker utfallet av beslutningstakingen i vesentlig grad, forstås som et KI-SYSTEM som ikke har innvirkning på innholdet i, og dermed utfallet av, beslutningstakingen, enten den er menneskelig eller automatisert. et KI-system som ikke påvirker utfallet av beslutningstakingen i vesentlig grad, kan omfatte situasjoner der ett eller flere av følgende vilkår er oppfylt. Det første vilkåret bør være at KI-systemet er ment å utføre en snever prosessuell oppgave, for eksempel et KI-SYSTEM som omdanner ustrukturerte data til strukturerte data, et KI-SYSTEM som klassifiserer innkommende dokumenter i kategorier eller et KI-system som brukes til å oppdage duplikater blant et stort antall applikasjoner. Disse oppgavene er av en så snever og begrenset art at de bare utgjør en begrenset risiko som ikke økes ved bruk AV et aI-system i en sammenheng som er oppført som høyrisikobruk i et vedlegg til denne forordning. Den andre betingelsen bør være

(30) Europaparlaments- og rådsforordning (EU) 2018/1139 av 4. juli 2018 om felles regler for sivil luftfart og om opprettelse av Den europeiske unions byrå for luftfartssikkerhet, og om endring av forordning (EF) nr. 2111/2005, (EF) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 og europaparlaments- og rådsdirektiv 2014/30/EU og 2014/53/EU, og om oppheving av europaparlaments- og rådsforordning (EF) nr. 552/2004 og (EF) nr. 216/2008 og rådsforordning (EØF) nr. 3922/91 (EUT L 212 av 22.8.2018, p. 1).

(31) Europaparlaments- og rådsforordning (EU) 2019/2144 av 27. november 2019 om krav til typegodkjenning av motorvogner og tilhengere til disse, og systemer, komponenter og separate tekniske enheter beregnet på slike kjøretøyer, med hensyn til deres generelle sikkerhet og beskyttelse av kjøretøyets passasjerer og myke trafikanter, om endring av europaparlaments- og rådsforordning (EU) 2018/858 og om oppheving av forordning (EF) nr. 78/2009, (EF) nr. 79/2009 og (EF) nr. 661/2009 og kommisjonsforordning (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. 1008/2010, (EU) nr. 1009/2010, (EUnr. 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 av 16.12.2019, p. 1).

at oppgaven som utføres AV aI-systemet, er ment å forbedre resultatet av en tidligere utført menneskelig aktivitet som kan relevant for som er oppført i et vedlegg til denne forordning. Med tanke på disse egenskapene gir aI-systemet bare et ekstra lag til en menneskelig aktivitet med følgelig lavere risiko. Dette vilkåret vil for eksempel gjelde for aI-systemer som er ment å forbedre språket som brukes i tidligere utarbeidede dokumenter, for eksempel i forhold til profesjonell tone, akademisk eller ved å tilpasse teksten til et bestemt merkevarebudskap. Det tredje vilkåret bør være at KI-systemet har til hensikt å oppdage beslutningsmønstre eller avvik fra tidligere beslutningsmønstre. Risikoen reduseres fordi bruken av AI-SYSTEMET følger en tidligere gjennomført menneskelig vurdering, som det ikke er ment å erstatte eller påvirke, uten en skikkelig menneskelig gjennomgang. Slike aI-systemer kan for eksempel brukes til å sjekke i *ettertid* om en lærer har avveket fra *et* bestemt vurderingsmønster, slik at potensielle inkonsekvenser eller avvik kan fanges opp. Det fjerde vilkåret bør være at KI-systemet er beregnet på å utføre en oppgave som bare er forberedende for en vurdering som ER relevant for formålene med KI-systemene oppført i et vedlegg til denne forordning, slik at den mulige virkningen av systemets resultater er svært liten når det gjelder å utgjøre en risiko for den påfølgende vurderingen. Dette vilkåret dekker blant annet smarte løsninger for filhåndtering, som omfatter ulike funksjoner fra indeksering, søk, tekst- og talebehandling eller kobling av data til andre datakilder, eller som brukes til oversettelse av originaldokumenter. Under alle omstendigheter bør aI-systemer som brukes i høyrisiko-brukstilfeller som er oppført i et vedlegg til denne forordning, anses å utgjøre en betydelig risiko for skade på helse, sikkerhet eller grunnleggende rettigheter dersom AI-SYSTEMET innebærer profilering I henhold til artikkel 4 nr. 4 i forordning (EU) 2016/679 eller artikkel 3 . 4 i direktiv (EU) 2016/680 eller artikkel 3 nr. 5 i forordning (EU) 2018/1725. For å sikre sporbarhet og åpenhet bør en leverandør som anser at ET KI-system ikke utgjør en høy risiko på grunnlag av vilkårene nevnt ovenfor, utarbeide dokumentasjon av vurderingen før systemet bringes i omsetning eller tas i bruk, og bør på anmodning utlevere denne dokumentasjonen til nasjonale vedkommende myndigheter. En slik leverandør bør være forpliktet til å registrere AI-systemet i EU-databasen som opprettes i henhold til denne forordning. For å gi ytterligere veiledning om den praktiske gjennomføringen av vilkårene for at aI-systemene som er oppført i et vedlegg til denne forordning, unntaksvis ikke utgjør høy risiko, bør Kommisjonen, etter å ha rådført seg med Personvernrådet, utarbeide retningslinjer som spesifiserer den praktiske gjennomføringen, supplert med en omfattende liste over praktiske eksempler på bruksområder FOR AI-SYSTEMER som utgjør høy risiko, og bruksområder som ikke gjør det.

(54) ettersom biometriske data utgjør en spesiell kategori av personopplysninger, er det hensiktsmessig å klassifisere flere tilfeller av kritisk bruk av biometriske systemer som høyrisiko, i den grad bruken av dem er tillatt i henhold til relevant unionsrett og nasjonal rett. Tekniske unøyaktigheter I AI-systemer beregnet på biometrisk fjernidentifikasjon av fysiske personer kan føre skjeve resultater og ha diskriminerende virkninger. Risikoen for slike skjeve resultater og diskriminerende virkninger er særlig relevant med hensyn til alder, etnisitet, rase, kjønn eller nedsatt funksjonsevne. Systemer for fjernstyrt biometrisk identifikasjon bør derfor klassifiseres som høyrisikosystemer med tanke på den risikoen de utgjør. En slik klassifisering utelukker KI-systemer som er beregnet på å brukes til biometrisk verifisering, herunder autentisering, hvis eneste formål er å bekrefte at en bestemt fysisk person er den vedkommende utgir seg for å være, og å bekrefte identiteten til en fysisk person med det ene formål å få tilgang til en tjeneste, låse opp en enhet eller få sikker tilgang til lokaler. I tillegg bør AI-SYSTEMER som er beregnet på å brukes til biometrisk kategorisering i henhold til sensitive attributter eller kjennetegn som er beskyttet i henhold til artikkel 9 nr. 1 i forordning (EU) 2016/679 på grunnlag av biometriske data, i den grad disse ikke er forbudt i henhold til denne forordning, og systemer for følelsesgjenkjenning som ikke er forbudt i henhold til denne forordning, klassifiseres som høyrisikosystemer. Biometriske systemer som utelukkende er ment å brukes for å muliggjøre cybersikkerhets- og personopplysningsverntiltak, bør ikke anses som høyrisikosystemer FOR AI.

(55) Når det gjelder forvaltning og drift av kritisk infrastruktur, er det hensiktsmessig å klassifisere KI-systemene som er beregnet på Å brukes som sikkerhetskomponenter i forvaltningen og driften av kritisk digital infrastruktur som oppført i nr. 8 I vedlegget til direktiv (EU) 2022/2557, veitrafikk og vann-, gass-, varme- og elektrisitetsforsyning, som høyrisikosystemer, siden svikt eller funksjonsfeil i dem kan sette menneskers liv og helse i fare I stort omfang og føre til betydelige forstyrrelser i den ordinære utøvelsen av sosial og økonomisk virksomhet. Sikkerhetskomponenter i kritisk infrastruktur, herunder kritisk digital infrastruktur, er systemer som brukes til direkte å beskytte fysiske integriteten til kritisk infrastruktur eller helse og sikkerhet personer og eiendom, men som ikke er nødvendige for at den kritiske infrastrukturen skal kunne fungere.

systemet for å fungere. Svikt eller funksjonsfeil i slike komponenter kan direkte føre til risiko for den fysiske integriteten til kritisk infrastruktur og dermed til risiko for helse og sikkerhet for personer og eiendom. Komponenter som utelukkende skal brukes til cybersikkerhetsformål, bør ikke kvalifisere som sikkerhetskomponenter. Eksempler på sikkerhetskomponenter i slik kritisk infrastruktur kan være systemer for overvåking av vanntrykk eller brannvarslingsanlegg i skytjenester.

(56) Det er viktig Å ta i BRUK aI-systemer I utdanningen for å fremme digital utdanning og opplæring av høy kvalitet og for å gjøre det mulig for alle elever og lærere å tilegne seg og dele de nødvendige digitale ferdighetene og kompetansene, herunder mediekompetanse og kritisk tenkning, slik at de kan delta aktivt i økonomien, samfunnet og i demokratiske prosesser. aI-systemer som brukes I utdanning eller yrkesopplæring, særlig for å bestemme tilgang eller opptak, for å tildele personer til utdannings- og yrkesopplæringsinstitusjoner eller -programmer på alle nivåer, for å evaluere læringsutbyttet til personer, for å vurdere hvilket som er passende for en person, og som i vesentlig grad påvirker det utdannings- og opplæringsnivået som enkeltpersoner vil få eller vil kunne få tilgang til, eller for å overvåke og avdekke ulovlig atferd hos studenter under prøver, bør klassifiseres som høyrisikosystemer FOR AI, siden de kan være avgjørende for en persons utdannings- og yrkesliv og derfor kan påvirke denne personens mulighet til å sikre seg et levebrød. Når slike systemer ikke er utformet og brukes på riktig måte, kan de være særlig inngripende og krenke retten til utdanning og opplæring samt retten til ikke å bli diskriminert, og videreføre historiske diskrimineringsmønstre, for eksempel mot kvinner, visse aldersgrupper, personer med nedsatt funksjonsevne, personer av en bestemt rase eller etnisk opprinnelse eller personer med en bestemt seksuell legning.

(57) AI systemer som brukes i forbindelse med ansettelse, arbeidsledelse og adgang til selvstendig næringsvirksomhet, særlig for rekruttering og utvelgelse av personer, for å treffe beslutninger som påvirker vilkårene for arbeidsforholdet, forfremmelse og avslutning av arbeidsrelaterte , for å fordele oppgaver på grunnlag av individuell atferd, personlige egenskaper eller kjennetegn og for å overvåke eller evaluere personer i arbeidsrelaterte kontraktsforhold, bør også klassifiseres som høyrisikosystemer, siden disse systemene kan ha en betydelig innvirkning på fremtidige karrieremuligheter, disse personenes levebrød og arbeidstakernes rettigheter. Relevante arbeidsrelaterte kontraktsforhold bør på en meningsfull måte involvere ansatte og personer som tilbyr tjenester gjennom plattformer som nevnt i Kommisjonens arbeidsprogram for 2021. Gjennom hele rekrutteringsprosessen og i evalueringen, forfremmelsen eller beholdningen av personer i arbeidsrelaterte kontraktsforhold kan slike systemer videreføre historiske diskrimineringsmønstre, for eksempel mot kvinner, visse aldersgrupper, personer med nedsatt funksjonsevne eller personer av en bestemt rase, etnisk opprinnelse eller seksuell legning. aI-systemer som brukes til å overvåke prestasjonene og atferden til slike personer, kan også undergrave deres grunnleggende rettigheter til databeskyttelse og personvern.

(58) et annet område der bruken AV AI-systemer fortjener spesiell oppmerksomhet, er tilgangen til og nytten av visse viktige private og offentlige tjenester og ytelser som er nødvendige for at folk skal kunne delta fullt ut samfunnet eller forbedre sin levestandard. Særlig er fysiske personer som søker om eller mottar viktige offentlige ytelser og tjenester fra offentlige myndigheter, nemlig helsetjenester, trygdeytelser, sosiale tjenester som gir beskyttelse i tilfeller som svangerskap, sykdom, arbeidsulykker, avhengighet eller alderdom og tap av arbeid, samt sosialhjelp og bostøtte, typisk avhengige av disse ytelsene og tjenestene og i en sårbar posisjon i forhold til de ansvarlige myndighetene. Dersom AI-systemer brukes for å avgjøre om slike ytelser og tjenester bør innvilges, avslås, reduseres, tilbakekalles eller kreves tilbake av myndighetene, herunder om mottakerne har rettmessig krav på slike ytelser eller tjenester, kan disse systemene ha en betydelig innvirkning på personers levebrød og kan krenke deres grunnleggende rettigheter, som retten til sosial beskyttelse, ikke-diskriminering, menneskeeller et effektivt rettsmiddel, og bør derfor klassifiseres som høyrisiko. Denne forordning bør likevel ikke hindre utviklingen og bruken av innovative tilnærminger i den offentlige forvaltningen, som vil kunne dra nytte av en mer bruk av kompatible og sikre aI-systemer, forutsatt at disse systemene ikke innebærer en høy risiko for juridiske og fysiske personer. I tillegg bør aI-systemer som brukes til å vurdere fysiske personers kredittverdighet eller kredittverdighet, klassifiseres som høyrisikosystemer, siden de avgjør disse personenes tilgang til økonomiske ressurser eller viktige tjenester som bolig, elektrisitet og . aI-systemer som brukes til disse formålene, kan føre til diskriminering mellom personer eller grupper og kan videreføre historiske diskrimineringsmønstre, for eksempel på grunnlag av rase eller etnisk opprinnelse, kjønn, funksjonshemming, alder eller seksuell legning, eller kan skape nye former for diskriminerende virkninger. KI-systemer som er fastsatt I unionsretten med det formål å avdekke svindel i forbindelse med tilbud av finansielle tjenester og for tilsynsmessige formål for å beregne kredittinstitusjoners og forsikringsselskapers kapitalkrav, bør imidlertid ikke anses som høyrisikosystemer i henhold til denne forordning. Videre bør alle systemer SOM er beregnet på

som skal brukes risikovurdering og prising i forhold til fysiske personer for helse- og livsforsikring, kan også ha en betydelig innvirkning på personers levebrød, og hvis de ikke utformes, utvikles og brukes på riktig måte, kan de krenke deres grunnleggende rettigheter og føre til alvorlige konsekvenser for menneskers liv og helse, inkludert økonomisk ekskludering og diskriminering. Endelig bør AI-systemer som brukes til å evaluere og klassifisere fra fysiske personer eller til å sende ut eller fastsette prioritet ved utsendelse av førstehjelpstjenester, inkludert politi, brannmenn og medisinsk hjelp, samt systemer for triagering av akuttpasienter I helsevesenet, også klassifiseres som høyrisikosystemer, siden de tar beslutninger i situasjoner som er svært kritiske for menneskers liv og helse og deres eiendom.

(59) Gitt deres rolle og ansvar, rettshåndhevelsesmyndighetenes handlinger som involverer visse former for bruk AV aI-systemer, preget av en betydelig grad av maktubalanse og kan føre til overvåking, pågripelse eller frihetsberøvelse av en fysisk person, samt andre negative konsekvenser for de grunnleggende rettighetene som er garantert i pakten. Særlig hvis AI-systemet ikke er opplært med data av høy kvalitet, ikke oppfyller tilstrekkelige krav til ytelse, nøyaktighet eller robusthet, eller ikke er utformet og testet på riktig måte før det markedsføres eller på annen måte tas i bruk, kan det skille ut personer på en diskriminerende eller på annen måte uriktig eller urettferdig måte. Videre kan utøvelsen av viktige grunnleggende prosessuelle rettigheter, som retten til ET effektivt rettsmiddel og til en rettferdig rettergang, samt retten til forsvar og uskyldspresumsjonen, bli hindret, særlig dersom slike systemer ikke er tilstrekkelig gjennomsiktige, forklarlige og dokumenterte. Det er derfor hensiktsmessig å klassifisere en rekke AI-systemer som er ment å brukes i rettshåndhevelsessammenheng, der nøyaktighet, pålitelighet og åpenhet er særlig viktig for å unngå negative konsekvenser, bevare allmennhetens tillit og sikre ansvarlighet og effektiv oppreisning, som høyrisikosystemer, i den grad bruken AV dem ER tillatt i henhold til relevant og nasjonal rett. I lys av virksomhetens art og risikoene forbundet med den, bør disse høyrisikosystemene for KUNSTIG INTELLIGENS særlig omfatte systemer KUNSTIG INTELLIGENS som er beregnet på å brukes av eller på vegne av rettshåndhevelsesmyndigheter eller av unionsinstitusjoner, -organer, -kontorer eller -byråer til støtte for rettshåndhevelsesmyndigheter for å vurdere risikoen for at en fysisk person kan bli offer for straffbare handlinger, som løgndetektorer og lignende verktøy, for å vurdere påliteligheten av bevis i forbindelse etterforskning eller straffeforfølgning av straffbare handlinger, og, i den grad det ikke er forbudt i henhold til denne forordning, for å vurdere risikoen for at en fysisk person begår lovbrudd eller begår nye lovbrudd, ikke utelukkende på grunnlag av profilering av fysiske personer eller vurdering av personlighetstrekk og egenskaper eller tidligere kriminell atferd hos fysiske personer eller grupper, for profilering i forbindelse med avdekking, etterforskning eller straffeforfølgning av straffbare handlinger. aI-systemer som er spesielt beregnet på å brukes til administrativ saksbehandling av skatte- og tollmyndigheter samt av finansetterretningsenheter som utfører administrative oppgaver med å analysere informasjon i henhold til unionsretten om hvitvasking AV penger, bør ikke klassifiseres som høyrisiko aI-systemer som brukes av rettshåndhevelsesmyndigheter for å forebygge, avdekke, etterforske og straffeforfølge straffbare handlinger. Rettshåndhevelsesmyndighetenes og andre relevante myndigheters bruk av aI-verktøy bør ikke bli en faktor for ulikhet eller utestenging. Det bør ikke ses bort fra innvirkningen bruken AV aI-verktøy har på mistenktes rett til forsvar, særlig vanskelighetene med å få meningsfull informasjon hvordan disse systemene fungerer, og de påfølgende vanskelighetene med å bestride resultatene i retten, særlig for fysiske personer som er under etterforskning.

(60) AI-SYSTEMER som brukes i migrasjons-, asyl- og grensekontrollforvaltningen, berører personer som ofte er i en særlig sårbar posisjon og som er avhengige av resultatet av de kompetente offentlige myndighetenes handlinger. Nøyaktigheten, den ikke-diskriminerende karakteren og åpenheten til AI-SYSTEMENE som brukes i disse sammenhengene, er derfor særlig viktig for å garantere respekt for de grunnleggende rettighetene til de berørte personene, særlig deres rett til fri bevegelighet, ikke-diskriminering, beskyttelse av privatliv og personopplysninger, internasjonal beskyttelse og god administrasjon. Det er derfor hensiktsmessig å klassifisere som høyrisikosystemer, i DEN grad bruken av dem er tillatt I henhold til relevant unionsrett og nasjonal rett, systemer som er beregnet på Å brukes av eller på vegne av vedkommende offentlige myndigheter eller av unionsinstitusjoner, -organer, -kontorer eller -byråer med oppgaver på områdene migrasjon, asyl og grensekontrollforvaltning, som løgndetektorer og lignende verktøy, for å vurdere visse risikoer som fysiske personer som reiser inn på en medlemsstats territorium eller søker om visum eller asyl, utgjør, for å bistå vedkommende offentlige myndigheter i forbindelse med behandling, herunder vurdering av bevisenes pålitelighet, av søknader om asyl, visum og oppholdstillatelse og tilknyttede klager med hensyn til målet om å fastslå om de fysiske personene som søker om en status, er kvalifiserte, med det formål å oppdage, gjenkjenne eller identifisere fysiske personer i forbindelse med migrasjon, asyl og grensekontroll, med unntak av verifisering av reisedokumenter. aI-systemer på området migrasjon, asyl og grensekontroll som omfattes av denne forordning, bør oppfylle de relevante prosedyrekravene fastsatt i europaparlaments- og rådsforordning (EF) nr. 810/2009.

av Rådet ([32]), europaparlaments- og rådsdirektiv 2013/32/EU ([33])og annen relevant unionsrett. Bruken AV AI-systemer i migrasjons-, asyl- og grensekontrollforvaltningen bør ikke under noen omstendighet brukes av medlemsstatene eller Unionens institusjoner, organer, kontorer eller byråer som et middel til å omgå deres internasjonale forpliktelser i henhold til FN-konvensjonen om flyktningers status, undertegnet i Genève 28. juli 1951, som endret ved protokollen av 31. januar 1967. De skal heller ikke brukes til på noen måte å krenke prinsippet om non-refoulement, eller til å nekte trygge og effektive lovlige veier inn Unionens territorium, herunder retten til internasjonal beskyttelse.

(61) Visse KI-SYSTEMER som er beregnet på rettspleie og demokratiske prosesser, bør klassifiseres som høyrisikosystemer, med tanke på deres potensielt betydelige innvirkning på demokratiet, rettsstaten, individuelle friheter samt retten til et effektivt rettsmiddel og til en rettferdig rettergang. For å håndtere risikoen for potensielle skjevheter, feil og ugjennomsiktighet er det særlig hensiktsmessig å klassifisere AI-systemer som er ment å brukes av en rettslig myndighet eller på dens vegne for å bistå rettslige myndigheter med å undersøke og tolke fakta og jussen, og med å anvende jussen på et konkret sett med fakta, som høyrisikosystemer. AI-systemer som er ment å brukes av alternative tvisteløsningsorganer for disse formålene, bør også anses som høyrisikosystemer når utfallet av den alternative tvisteløsningen får rettsvirkninger for partene. Bruken AV aI-verktøy kan støtte dommernes beslutningsmakt eller domstolenes uavhengighet, men bør ikke erstatte den: Den endelige beslutningstakingen må fortsatt være en menneskestyrt aktivitet. Klassifiseringen AV aI-systemer som høyrisikosystemer bør imidlertid ikke omfatte aI-systemer som er beregnet på rent administrative tilleggsaktiviteter som ikke påvirker den faktiske rettspleien i enkeltsaker, for eksempel anonymisering eller pseudonymisering av rettsavgjørelser, dokumenter eller data, kommunikasjon mellom ansatte og administrative oppgaver.

(62) Uten at det berører reglene i europaparlaments- og rådsforordning (EU) 2024/900 ([34]), og for å håndtere risikoen for utilbørlig ekstern innblanding i stemmeretten som er nedfelt i artikkel 39 i pakten, og for negative virkninger på demokratiet og rettsstaten, bør AI-systemer som er ment å brukes å påvirke utfallet av et valg eller en folkeavstemning eller fysiske personers stemmegivning ved valg eller folkeavstemninger, klassifiseres som høyrisikosystemer, med unntak av AI-SYSTEMER som fysiske personer ikke er direkte eksponert for, for eksempel verktøy som brukes til å organisere, optimalisere og strukturere politiske kampanjer fra et administrativt og logistisk synspunkt.

(63) Det faktum at et KI-SYSTEM er klassifisert som et høyrisikosystem FOR KI I henhold til denne forordning, bør ikke tolkes som en indikasjon på at bruken av systemet er lovlig i henhold til andre unionsrettsakter eller i henhold til nasjonal rett som er forenlig med , f.eks. om vern AV personopplysninger, om bruk av løgndetektorer og lignende verktøy eller andre systemer for å avdekke fysiske personers følelsesmessige tilstand. slik bruk bør fortsatt skje utelukkende i samsvar med gjeldende krav som følger av pakten og av gjeldende sekundærrettsakter i unionsretten og nasjonal rett. Denne forordning bør ikke forstås slik at den gir rettslig grunnlag for behandling av personopplysninger, herunder særlige kategorier av personopplysninger, der det er relevant, med mindre annet er uttrykkelig fastsatt i denne forordning.

(64) For å redusere risikoen ved høyrisiko-ai-systemer som bringes i omsetning eller tas i bruk, og for å sikre høy grad av pålitelighet, bør visse obligatoriske krav gjelde for HØYRISIKO-AI-SYSTEMER, idet det tas hensyn til det tiltenkte formålet med og brukssammenhengen for aI-systemet og i samsvar med det risikohåndteringssystemet som skal etableres av leverandøren. Tiltakene som leverandørene treffer for å oppfylle de obligatoriske kravene i denne forordning, bør ta hensyn til den allment anerkjente kunnskapsstatus om AI, være forholdsmessige og effektive for å oppfylle målene i denne forordning. På grunnlag av det nye lovgivningsrammeverket, som klargjort i Kommisjonens kunngjøring "The "Blue Guide" on the implementation of EU product rules 2022", er den generelle regelen at mer enn én rettsakt i Unionens harmoniseringslovgivning kan få anvendelse på ett produkt, siden tilgjengeliggjøring eller ibruktaking bare kan finne sted når produktet er i samsvar med all gjeldende harmoniseringslovgivning i Unionen. Farene ved AI-systemer som omfattes av kravene i denne forordningen, gjelder andre aspekter enn den eksisterende EU-harmoniseringslovgivningen, og kravene i denne forordningen vil derfor utfylle den eksisterende EU-harmoniseringslovgivningen. For eksempel kan maskiner eller medisinsk utstyr som inneholder et AI-SYSTEM, innebære risikoer som ikke er omfattet av de grunnleggende helse- og sikkerhetskravene.

(32) Europaparlaments- og rådsforordning (EF) nr. 810/2009 av 13. juli 2009 om innføring av en fellesskapskodeks for visum (visakodeks) (EUT L 243 av 15.9.2009, s. 1).

(33) Europaparlaments- og rådsdirektiv 2013/32/EU av 26. juni 2013 om felles prosedyrer for innvilgelse og tilbaketrekking av internasjonal beskyttelse (EUT L 180 av 29.6.2013, s. 60).

(34) Europaparlaments- og rådsforordning (EU) 2024/900 av 13. mars 2024 om åpenhet og målretting av politisk reklame (EUT L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj).

kravene i den relevante harmoniserte EU-lovgivningen, ettersom denne sektorlovgivningen ikke omhandler risikoer som er spesifikke for AI-systemer. Dette krever en samtidig og utfyllende anvendelse av de ulike rettsaktene. For å sikre konsekvens og unngå unødvendige administrative byrder og unødvendige kostnader bør leverandører av et produkt som inneholder ett eller flere høyrisikosystemer for KUNSTIG intelligens, som omfattes av kravene i denne forordning og i Unionens harmoniseringslovgivning basert på den nye rettslige rammen og oppført i et vedlegg til denne forordning, ha fleksibilitet med hensyn til operasjonelle beslutninger om hvordan de skal sikre at et produkt som inneholder ett eller flere systemer for KUNSTIG INTELLIGENS, oppfyller alle gjeldende krav i den harmoniserte unionslovgivningen på best mulig måte. Denne fleksibiliteten kan for eksempel innebære at leverandøren kan beslutte å integrere en del av de nødvendige test- og rapporteringsprosessene, opplysningene og dokumentasjonen som kreves i henhold til denne forordning, i allerede eksisterende dokumentasjon og framgangsmåter som kreves i henhold til eksisterende harmonisert unionslovgivning basert på den nye rettslige rammen og oppført i et vedlegg til denne forordning. Dette skal ikke på noen måte undergrave leverandørens plikt til å overholde alle gjeldende krav.

(65) Risikohåndteringssystemet bør bestå av en kontinuerlig, iterativ prosess som planlegges og gjennomføres gjennom hele livssyklusen til et . Prosessen bør ha som mål å identifisere og redusere de relevante risikoene et AI-SYSTEM utgjør for helse, sikkerhet og grunnleggende rettigheter. Risikohåndteringssystemet bør gjennomgås og oppdateres regelmessig for å sikre at det fortsatt er effektivt, og at alle viktige beslutninger og tiltak som treffes i henhold til denne forordning, begrunnes og dokumenteres. Denne prosessen bør sikre at leverandøren identifiserer risikoer eller negative virkninger og iverksetter risikoreduserende tiltak for kjente og rimelig forutsigbare risikoer som KI-systemene utgjør for helse, sikkerhet og grunnleggende rettigheter, i lys av deres tiltenkte formål og rimelig forutsigbar feilbruk, herunder mulige risikoer som oppstår som følge av samspillet MELLOM KI-SYSTEMET og miljøet der det opererer. Risikohåndteringssystemet bør ta i bruk de mest hensiktsmessige risikohåndteringstiltakene I lys av DEN nyeste kunnskapen innen KI. Ved identifisering av de mest hensiktsmessige risikohåndteringstiltakene bør leverandøren dokumentere og forklare de valgene som er gjort, og, når det er relevant, involvere eksperter og eksterne interessenter. Ved identifisering av rimelig forutsigbar feilbruk AV høyrisiko , bør leverandøren dekke bruk av aI-systemer som, selv om de ikke er direkte dekket av det tiltenkte formålet og fastsatt i bruksanvisningen, likevel med rimelighet kan forventes å være et resultat av lett forutsigbar menneskelig atferd i sammenheng med de spesifikke egenskapene og bruken av et bestemt aI-system. alle kjente eller forutsigbare omstendigheter knyttet til bruken AV HØYRISIKO-AI-SYSTEMET i samsvar med det tiltenkte formålet eller under forhold med rimelig forutsigbar feilbruk, som kan føre til risiko for helse og sikkerhet eller grunnleggende rettigheter, bør inkluderes i bruksanvisningen som leveres av leverandøren. Dette for å sikre at brukeren er klar over og tar hensyn til disse når han eller hun bruker høyrisiko-AI-systemet. Identifisering og gjennomføring av risikoreduserende tiltak for påregnelig misbruk i henhold til denne forordningen bør ikke kreve at leverandøren gir spesifikk I høyrisiko-ai-systemet for å håndtere påregnelig misbruk. Tilbyderne oppfordres imidlertid til å vurdere slike ytterligere opplæringstiltak for å redusere rimelig forutsigbar feilbruk der det er nødvendig og hensiktsmessig.

(66) Det bør stilles krav til høyrisiko-AI-systemer når det gjelder risikohåndtering, kvaliteten og relevansen av datasettene som brukes, teknisk dokumentasjon og journalføring, åpenhet og informasjon til distributører, menneskelig tilsyn samt robusthet, nøyaktighet og cybersikkerhet. Disse kravene er nødvendige for effektivt å redusere risikoen for helse, sikkerhet og grunnleggende rettigheter. ettersom det ikke finnes andre mindre handelsbegrensende tiltak som med rimelighet er tilgjengelige, er disse kravene ikke ubegrunnede handelsrestriksjoner.

(67) Data av høy kvalitet og tilgang til data av høy kvalitet spiller en viktig rolle når det gjelder å skape struktur og sikre ytelsen til mange aI-systemer, særlig når det brukes teknikker som involverer opplæring AV modeller, med sikte på å sikre at høyrisiko aI-systemet fungerer som forutsatt og trygt, og at det ikke blir en kilde til diskriminering som er forbudt i henhold til unionsretten. Datasett av høy kvalitet for opplæring, validering og testing krever at det iverksettes egnede metoder for datastyring og -forvaltning. datasett for opplæring, validering og testing, inkludert etikettene, skal være relevante, tilstrekkelig representative og i størst mulig grad være feilfrie og fullstendige med tanke på systemets tiltenkte formål. For å gjøre det lettere å overholde EUs personvernlovgivning, for eksempel forordning (EU) 2016/679, bør praksis for datastyring og -forvaltning, når det gjelder personopplysninger, omfatte åpenhet om det opprinnelige formålet med datainnsamlingen. Datasettene bør også ha de nødvendige statistiske egenskapene, blant annet med hensyn til de personene eller gruppene av personer som høyrisikoanalysesystemet er ment å brukes på, med særlig vekt på å redusere mulige skjevheter i datasettene som kan påvirke personers helse og sikkerhet, ha en negativ innvirkning på grunnleggende rettigheter eller føre diskriminering som er forbudt i henhold til unionsretten, særlig der datautdata påvirker input for fremtidige operasjoner.

(tilbakekoblingssløyfer). Skjevheter kan for eksempel være iboende i de underliggende datasettene, særlig når historiske data brukes, eller de kan oppstå når systemene implementeres i den virkelige verden. Resultatene KI-systemer kan påvirkes av slike iboende skjevheter som gradvis kan øke dermed videreføre og forsterke eksisterende diskriminering, særlig for personer som tilhører visse utsatte grupper, inkludert rasemessige eller etniske grupper. Kravet om at datasettene i størst mulig grad skal være fullstendige og feilfrie, bør ikke påvirke bruken av personvernbevarende teknikker I forbindelse med utvikling og testing AV KI-systemer. Datasettene bør særlig, i den grad det er nødvendig ut fra det tiltenkte formålet, ta hensyn til de funksjonene, egenskapene eller elementene som er spesielle for den spesifikke geografiske, kontekstuelle, atferdsmessige eller funksjonelle settingen som aI-systemet er ment å bli brukt I. Kravene til datastyring kan oppfylles ved å benytte seg av tredjeparter som tilbyr sertifiserte samsvarstjenester, herunder verifisering av datastyring, datasettintegritet og praksis for opplæring, validering og testing av data, i den grad det sikres samsvar med datakravene i denne forordning.

(68) For utvikling og vurdering av høyrisikosystemer FOR kunstig INTELLIGENS bør visse aktører, f.eks. leverandører, meldte organer og andre relevante enheter, f.eks. europeiske digitale innovasjonssentre, test- og forsøksanlegg og forskere, kunne få tilgang til og bruke datasett av høy kvalitet innenfor disse aktørenes virksomhetsområder som er knyttet til denne forordning. Felles europeiske datarom som er opprettet av Kommisjonen, og tilrettelegging for datadeling mellom bedrifter og med myndighetene i allmennhetens interesse, vil være avgjørende for å gi pålitelig, ansvarlig og ikke-diskriminerende tilgang til data av høy kvalitet for opplæring, validering og testing av KI-systemer. For eksempel vil det europeiske helsedatarommet legge til rette for ikke-diskriminerende tilgang til helsedata og opplæring av aI-algoritmer på disse datasettene, på en måte som ivaretar personvernet, er sikker, rettidig, åpen og pålitelig, og med en hensiktsmessig institusjonell styring. Relevante kompetente myndigheter, herunder sektormyndigheter, som gir eller støtter tilgangen til data, kan også støtte levering av data av høy kvalitet for opplæring, validering og testing av aI-systemer.

(69) Retten til personvern og beskyttelse av personopplysninger må garanteres gjennom hele livssyklusen TIL aI-systemet. I denne forbindelse gjelder prinsippene om dataminimering og innebygd personvern og personvern som standardinnstilling, som fastsatt Unionens personvernlovgivning, når personopplysninger behandles. Tiltak som leverandører treffer for å sikre overholdelse av disse prinsippene, kan omfatte ikke bare anonymisering og kryptering, men også bruk av teknologi som gjør det mulig å bruke algoritmer på dataene og opplæring av aI-systemer uten overføring mellom parter eller kopiering av selve rådataene eller de strukturerte dataene, uten at det berører kravene om datastyring i denne forordning.

(70) For å beskytte andres rett til ikke å bli diskriminert som følge av skjevheter I AI-SYSTEMER, bør leverandørene unntaksvis, I grad det er strengt nødvendig for å sikre at skjevheter oppdages og korrigeres i forbindelse med aI-systemer med høy risiko, med forbehold om egnede garantier for fysiske personers grunnleggende rettigheter og friheter og etter anvendelse av alle gjeldende vilkår fastsatt i henhold til denne forordning i tillegg til vilkårene fastsatt i forordning (EU) 2016/679 og (EU) 2018/1725 og direktiv (EU) 2016/680, også kunne behandle særlige kategorier av personopplysninger, som et spørsmål av vesentlig interesse for allmennheten i henhold til artikkel 9 nr. 2 bokstav g) i forordning (EU) 2016/679 og artikkel 10 . 2 bokstav g) i (EU) 2018/1725.

(71) Det er avgjørende å ha forståelig informasjon om hvordan høyrisiko AI-SYSTEMER er utviklet og hvordan de fungerer gjennom hele sin levetid, for å muliggjøre sporbarhet av disse systemene, verifisere samsvar med kravene i denne forordning, samt overvåking av deres drift og overvåking etter at de er kommet på markedet. Dette krever at det føres registre og at det foreligger teknisk dokumentasjon som inneholder opplysninger som er nødvendige for å vurdere om KI-systemet ER I samsvar med de relevante kravene, og for å legge til rette for overvåking etter markedsføringen. Slik informasjon bør omfatte systemets generelle egenskaper, muligheter og begrensninger, algoritmer, data, opplæring, testing og valideringsprosesser som brukes, samt dokumentasjon om det relevante risikostyringssystemet, og være utformet på en klar og forståelig måte. Den tekniske dokumentasjonen bør holdes oppdatert gjennom hele aI-systemets levetid. Videre bør høYRISIKO-AI-SYSTEMER teknisk sett muliggjøre automatisk registrering av hendelser ved hjelp av logger i løpet av systemets levetid.

(72) For å løse problemene knyttet til ugjennomsiktighet og kompleksitet i visse AI-SYSTEMER og hjelpe driftsansvarlige med å oppfylle sine forpliktelser i henhold til denne forordning, bør det kreves åpenhet for med høy risiko før de i omsetning eller tas i bruk. Høyrisiko AI-SYSTEMER bør utformes på en måte som gjør det mulig for driftsansvarlige å forstå hvordan AI-SYSTEMET fungerer, evaluere dets funksjonalitet og forstå dets styrker og begrensninger. Høyrisiko AI-SYSTEMER bør ledsages av passende informasjon i form av bruksanvisninger. Slik informasjon bør omfatte aI-systemets egenskaper, muligheter og begrensningerDe bør omfatte informasjon om mulige kjente og forutsigbare omstendigheter knyttet til bruken AV , herunder tiltak fra brukerens SIDE som kan påvirke systemets virkemåte og ytelse, og som kan føre til risiko for helse, sikkerhet og grunnleggende rettigheter, om endringer som er forhåndsbestemt og samsvarsvurdert av leverandøren, og om relevante tiltak for menneskelig tilsyn, herunder tiltak for å gjøre det lettere for brukerne å tolke resultatene fra AI-SYSTEMET. Åpenhet, herunder den medfølgende bruksanvisningenskal hjelpe utrullerne med å bruke systemet og støtte dem i å ta informerte beslutninger. Utrullerne skal blant annet være bedre i stand til å velge riktig system i lys av de forpliktelsene som gjelder for dem, få informasjon om tiltenkt og utelukket bruk og bruke aI-systemet PÅ riktig måte og på en hensiktsmessig måte. For å gjøre informasjonen bruksanvisningen lettere å lese og lettere tilgjengelig, bør det, der det er hensiktsmessig, inkluderes illustrerende eksempler, for eksempel på begrensningene og på tiltenkt og utelukket bruk AV AI-SYSTEMET. Leverandørene bør sørge for at all dokumentasjon, inkludert bruksanvisningen, inneholder meningsfull, omfattende, tilgjengelig og forståelig informasjon som tar hensyn til behovene og den forutsigbare kunnskapen til dem som skal ta i bruk systemet. Bruksanvisningen bør gjøres tilgjengelig på et språk som lett kan forstås av dem som skal ta i bruk systemet, som fastsatt av den berørte medlemsstaten.

(73) Høyrisikosystemer FOR KUNSTIG INTELLIGENS bør utformes og utvikles på en slik måte at fysiske personer kan overvåke hvordan de fungerer, sikre at de brukes som forutsatt, og at konsekvensene av håndteres i løpet av systemets livssyklus. For å oppnå dette bør leverandøren av systemet identifisere egnede tiltak for menneskelig tilsyn før det markedsføres eller tas i bruk. Der det er hensiktsmessig, bør slike tiltak særlig garantere at systemet er underlagt innebygde driftsbegrensninger som ikke kan overstyres av systemet selv, og at det er lydhørt overfor den menneskelige operatøren, og at de fysiske personene som har fått tildelt menneskelig tilsyn, har nødvendig kompetanse, opplæring og myndighet til å utføre denne rollen. Det er også viktig å sikre at høyrisikosystemer for kunstig INTELLIGENS omfatter mekanismer som veileder og informerer en fysisk person som har fått tildelt menneskelig tilsyn, slik at vedkommende kan ta informerte beslutninger om, når og hvordan han eller hun skal gripe inn for å unngå negative konsekvenser eller risikoer, eller stoppe systemet dersom det ikke fungerer som forutsatt. Med tanke på de betydelige konsekvensene for personer dersom visse biometriske identifikasjonssystemer gir feil treff, bør det fastsettes et krav om utvidet menneskelig kontroll for disse systemene, slik at ingen handling eller beslutning kan treffes av den som tar i bruk systemet, på grunnlag av den identifikasjonen som systemet gir, med mindre dette har blitt særskilt kontrollert og bekreftet av minst to fysiske personer. Disse personene kan være fra en eller flere enheter og inkludere personen som opererer eller bruker systemet. Dette kravet bør ikke medføre unødvendige byrder eller forsinkelser, og det kan være tilstrekkelig at de separate bekreftelsene fra de ulike personene automatisk registreres i loggene som genereres av systemet. Gitt de særlige forholdene på områdene rettshåndhevelse, migrasjon, grensekontroll og asyl, bør dette kravet ikke få anvendelse dersom unionsretten eller nasjonal rett anser anvendelsen av dette kravet for å være uforholdsmessig.

(74) KI-systemer med høy risiko bør fungere konsekvent gjennom hele livssyklusen og oppfylle et passende nivå av nøyaktighet, robusthet og cybersikkerhet, i lys av deres tiltenkte formål og i samsvar med den allment anerkjente teknologiske utviklingen. Kommisjonen og relevante organisasjoner og interessenter oppfordres til å ta behørig hensyn til risikoreduksjon og negative konsekvenser av aI-systemet. Det forventede nivået av ytelsesmålinger bør oppgis i den medfølgende bruksanvisningen. Tilbyderne oppfordres til å kommunisere denne informasjonen til brukerne på en klar og lett forståelig måte, uten misforståelser eller villedende uttalelser. Unionens lovgivning om legal metrologi, herunder Europaparlamentets og Rådets direktiv 2014/31/EU ([35]) og 2014/32/EU ([36]), har som mål å sikre nøyaktigheten av målinger og bidra til åpenhet og rettferdighet i kommersielle transaksjoner. I denne sammenheng bør Kommisjonen, i samarbeid med relevante interessenter og organisasjoner, f.eks. metrologi- og målestokkmyndigheter, oppmuntre til utvikling av målestokker og målemetoder FOR AI-systemer, der det er hensiktsmessig. Kommisjonen bør i den forbindelse ta hensyn til og samarbeide med internasjonale partnere som arbeider med metrologi og relevante måleindikatorer knyttet til AI.

(35) Europaparlaments- og rådsdirektiv 2014/31/EU av 26. februar 2014 om harmonisering av medlemsstatenes lovgivning om tilgjengeliggjøring på markedet av ikke-automatiske vekter (EUT L 96 av 29.3.2014, s. 107).

(36) Europaparlaments- og rådsdirektiv 2014/32/EU av 26. februar 2014 om harmonisering av medlemsstatenes lovgivning om tilgjengeliggjøring på markedet av måleredskaper (EUT L 96 av 29.3.2014, s. 149).

(75) Teknisk robusthet er et sentralt krav til høyrisikosystemer. De skal være robuste i forhold til skadelig eller på annen måte uønsket atferd som kan skyldes begrensninger i systemene eller miljøet systemene opererer i (f.eks. feil, mangler, inkonsekvenser, uventede situasjoner). Derfor bør det treffes tekniske og organisatoriske tiltak for å sikre robustheten til høyrisikosystemer, for eksempel ved å utforme og utvikle egnede tekniske løsninger for å forhindre eller minimere skadelig eller på annen måte uønsket atferd. Disse tekniske løsningene kan for eksempel omfatte mekanismer som gjør det mulig for systemet å avbryte driften på en sikker måte (fail-safe-planer) når det oppstår visse avvik eller når driften foregår utenfor visse forhåndsbestemte grenser. Manglende beskyttelse mot disse risikoene kan føre til sikkerhetskonsekvenser eller påvirke de grunnleggende rettighetene negativt, for eksempel på grunn av feilaktige beslutninger eller eller partiske utdata generert AV KI-systemet.

(76) Cybersikkerhet spiller en avgjørende rolle når det gjelder å sikre at AI-SYSTEMER er motstandsdyktige mot forsøk på å endre bruken, oppførselen og ytelsen deres, eller at ondsinnede tredjeparter som utnytter systemets sårbarheter, kompromitterer sikkerhetsegenskapene. Cyberangrep mot KI-systemer kan utnytte KI-spesifikke ressurser, for eksempel opplæringsdatasett (f.eks. dataforgiftning) eller opplærte modeller (f.eks. kontradiktoriske angrep eller medlemsinferens), eller utnytte sårbarheter i KI-systemets digitale ressurser eller den underliggende IKT-infrastrukturen. For å sikre et cybersikkerhetsnivå som står i forhold til risikoen, bør leverandørene av høyrisikosystemer derfor iverksette egnede tiltak, for eksempel sikkerhetskontroller, som også tar hensyn til den underliggende IKT-infrastrukturen.

(77) Uten at det berører kravene til robusthet og nøyaktighet fastsatt i denne forordning, kan HØYRISIKO-AI-SYSTEMER som omfattes av en europaparlaments- og rådsforordning om horisontale cybersikkerhetskrav for produkter med digitale elementer i samsvar med nevnte forordning, påvise samsvar med cybersikkerhetskravene i denne forordning ved å oppfylle de grunnleggende cybersikkerhetskravene fastsatt i nevnte forordning. Når høyrisiko-AI-systemer oppfyller de grunnleggende kravene i en europaparlaments- og rådsforordning om horisontale cybersikkerhetskrav for produkter med digitale elementer, bør de anses å være I samsvar med cybersikkerhetskravene fastsatt i denne forordning I den oppfyllelsen av disse kravene er dokumentert i EU-samsvarserklæringen eller deler av denne som er utstedt i henhold til nevnte forordning. For dette formål bør vurderingen av cybersikkerhetsrisikoene knyttet til et produkt med digitale elementer som er klassifisert som et høyrisikosystem i henhold til denne forordning, utført I henhold til en europaparlaments- og rådsforordning om horisontale cybersikkerhetskrav for produkter med digitale elementer, ta hensyn til risikoer for et AI-systems cyberrobusthet med hensyn til forsøk fra uautoriserte tredjeparter på å endre dets bruk, virkemåte eller ytelse, herunder AI-spesifikke sårbarheter som dataforgiftning eller kontradiktoriske angrep, samt, i den grad det er relevant, risikoer for grunnleggende rettigheter i henhold til kravene i denne forordning.

(78) Prosedyren for samsvarsvurdering fastsatt i denne forordning bør få anvendelse på de grunnleggende cybersikkerhetskravene til et produkt med digitale elementer som omfattes av en europaparlaments- og rådsforordning om horisontale cybersikkerhetskrav for produkter med digitale elementer, og som er klassifisert SOM ET høyrisiko-AI-system I henhold til denne forordning. Denne regelen bør imidlertid ikke føre til en reduksjon av det nødvendige sikkerhetsnivået for kritiske produkter med digitale elementer som omfattes av en europaparlaments- og rådsforordning om horisontale cybersikkerhetskrav for produkter med digitale elementer. Som unntak fra denne regelen ER høyrisiko-AI-systemer som omfattes av denne forordning, og som også er kvalifisert som viktige og kritiske produkter med digitale elementer I henhold til en europaparlaments- og rådsforordning om horisontale cybersikkerhetskrav for produkter med digitale elementer, og som omfattes av framgangsmåten for samsvarsvurdering basert på internkontroll fastsatt i et vedlegg til denne forordning, derfor underlagt bestemmelsene om samsvarsvurdering i en europaparlaments- og rådsforordning om horisontale cybersikkerhetskrav for produkter med digitale elementer, for så vidt gjelder de grunnleggende cybersikkerhetskravene i nevnte forordning. I så fall bør de respektive bestemmelsene om samsvarsvurdering basert på internkontroll fastsatt i et vedlegg til denne forordning få anvendelse på alle andre aspekter som omfattes av denne forordning. På grunnlag av kunnskapen og ekspertisen I ENISA om cybersikkerhetspolitikken og oppgavene som er tillagt ENISA i henhold til europaparlaments- og rådsforordning (EU) 2019/881 ([37]), bør Kommisjonen samarbeide med ENISA om spørsmål knyttet til cybersikkerhet FOR KI-systemer.

(37) Europaparlaments- og rådsforordning (EU) 2019/881 av 17. april 2019 om ENISA (Den europeiske unions byrå for cybersikkerhet) og om cybersikkerhetssertifisering av informasjons- og kommunikasjonsteknologi og om oppheving av forordning (EU) nr. 526/2013 (cybersikkerhetsloven) (EUT L 151 av 7.6.2019, s. 15).

(79) Det er hensiktsmessig at en bestemt fysisk eller juridisk person, definert som leverandør, tar ansvaret for markedsføringen eller ibruktakelsen AV ET høyrisiko-AI-system, uavhengig av den fysiske eller juridiske personen er den som har utformet eller utviklet systemet.

(80) som signatarer av FN-konvensjonen om rettighetene til personer med nedsatt funksjonsevne er Unionen og medlemsstatene rettslig forpliktet til å beskytte personer med nedsatt funksjonsevne mot diskriminering og fremme likestilling, til å sikre at personer med nedsatt funksjonsevne har tilgang til informasjons- og kommunikasjonsteknologi og -systemer på lik linje med andre, og til å sikre respekt for personvernet for personer med nedsatt funksjonsevne. Med tanke på økende betydningen og bruken av INFORMASJONS- og kommunikasjonsteknologi, bør prinsippene om universell utforming anvendes på alle nye teknologier og tjenester for å sikre full og lik tilgang for alle som kan bli berørt av eller bruke informasjons- OG kommunikasjonsteknologi, inkludert personer med nedsatt funksjonsevne, på en måte som tar fullt hensyn til deres iboende verdighet og mangfold. Det er derfor avgjørende at leverandørene sikrer full overholdelse av tilgjengelighetskravene, herunder Europaparlamentets og Rådets direktiv (EU) 2016/2102 ([38]) og direktiv (EU) 2019/882. Tilbydere bør sikre samsvar med disse kravene gjennom design. Derfor bør de nødvendige tiltakene integreres så mye som mulig i utformingen av høyrisiko-AI-systemet.

(81) Leverandøren bør etablere et forsvarlig kvalitetsstyringssystem, sikre at den nødvendige framgangsmåten for samsvarsvurdering gjennomføres, utarbeide relevant dokumentasjon og etablere et solid system for overvåking etter at utstyret er brakt i omsetning. Tilbydere AV høyrisikosystemer FOR kunstig INTELLIGENS SOM er underlagt forpliktelser med hensyn til i henhold til relevant sektorspesifikk unionsrett, bør ha mulighet til å inkludere elementene i kvalitetsstyringssystemet fastsatt I denne forordning som en del av det eksisterende kvalitetsstyringssystemet fastsatt i den andre sektorspesifikke unionsretten. Komplementariteten mellom denne forordning og eksisterende sektorspesifikk unionsrett bør også tas i betraktning i framtidig standardiseringsvirksomhet eller veiledning vedtatt av Kommisjonen. Offentlige myndigheter som tar i bruk høyrisikosystemer for eget bruk, kan vedta og gjennomføre reglene for kvalitetsstyringssystemet som en del av det kvalitetsstyringssystemet som er vedtatt på nasjonalt eller regionalt plan, alt etter hva som er hensiktsmessig, idet det tas hensyn til sektorens særtrekk og den berørte offentlige myndighets kompetanse og organisasjon.

(82) For å muliggjøre håndheving av denne forordning og skape like vilkår for operatører, og idet det tas hensyn til de ulike formene for tilgjengeliggjøring av digitale produkter, er det viktig å sikre at en person som ER etablert i Unionen, under alle omstendigheter kan gi myndighetene all nødvendig informasjon om et aI-system ER I samsvar med kravene. Derfor bør tilbydere som er etablert i tredjestater, før de gjør sine aI-systemer tilgjengelige i Unionen, ved skriftlig fullmakt utpeke en autorisert representant som er etablert i Unionen. Denne representanten spiller en sentral rolle når det gjelder å sikre samsvar for høyrisikosystemer som bringes i omsetning eller tas i bruk i Unionen av leverandører som ikke er etablert i Unionen, og når det gjelder å fungere som kontaktperson for dem som er etablert i Unionen.

(83) I lys av arten og kompleksiteten av verdikjeden for AI-SYSTEMER og i tråd med den nye rettslige rammen er det avgjørende å sikre rettssikkerhet og gjøre det lettere å overholde denne forordningen. Derfor det nødvendig å klargjøre rollen og de spesifikke forpliktelsene til relevante operatører i denne verdikjeden, for eksempel importører og distributører som kan bidra til utviklingen av aI-systemer. I visse situasjoner kan disse aktørene opptre i mer enn én rolle samtidig og bør derfor kumulativt oppfylle alle relevante forpliktelser knyttet til disse rollene. For eksempel kan en aktør opptre som distributør og importør samtidig.

(84) For å sikre rettssikkerheten er det nødvendig å klargjøre at enhver distributør, importør, distributør eller annen tredjepart på visse særlige vilkår bør anses for å være leverandør av et høyrisiko-AI-system og derfor påta seg alle relevante forpliktelser. Dette vil være tilfelle dersom denne parten setter sitt navn eller varemerke på et høyrisiko AI-SYSTEM som allerede er brakt i omsetning eller tatt i bruk, uten at det berører kontraktsmessige ordninger som fastsetter at forpliktelsene skal fordeles på annen måte. Dette vil også være tilfelle dersom parten foretar en vesentlig endring av ET høyrisiko-AI-system som allerede er brakt i omsetning eller tatt i bruk, på en slik måte at det forblir et HØYRISIKO-AI-SYSTEM i samsvar med denne forordning, eller dersom den endrer det tiltenkte formålet med et AI-SYSTEM, herunder et AI-SYSTEM til allmenn bruk, som ikke er klassifisert som høyrisikosystem og som allerede er brakt I omsetning eller tatt i bruk, PÅ en slik måte at AI-SYSTEMET blir et høyrisiko-AI-system i samsvar med denne forordning. Disse bestemmelsene bør få anvendelse uten at det berører mer spesifikke bestemmelser som er fastsatt i visse harmoniseringsrettsakter fra Unionen på grunnlag av den nye rettslige rammen, som denne forordning sammen med

(38) Europaparlaments- og rådsdirektiv (EU) 2016/2102 av 26. oktober 2016 om tilgjengeligheten av offentlige organers nettsteder og mobilapplikasjoner (EUT L 327 av 2.12.2016, s. 1).

Forordningen bør gjelde. For eksempel bør artikkel 16 nr. 2 i forordning (EU) 2017/745, som fastsetter at visse endringer ikke skal anses som modifikasjoner av et utstyr som kan påvirke dets samsvar med gjeldende krav, fortsatt få anvendelse PÅ høyrisiko-AI-systemer som er medisinsk utstyr I til nevnte forordning.

(85) Allsidige aI-systemer kan brukes som høyrisiko aI-systemer i seg selv eller være komponenter i andre høyrisiko aI-systemer. På grunn av deres særlige art og for å sikre en rettferdig ansvarsfordeling I aI-verdikjeden bør derfor leverandørene av slike systemer, uavhengig av om de kan brukes som høyrisiko-ai-systemer I seg selv av andre leverandører eller som komponenter i høyrisiko-ai-systemer, og med mindre annet er fastsatt i denne forordning, samarbeide tett med leverandørene av de relevante høyrisiko-ai-systemene for å sikre at de overholder de relevante forpliktelsene i henhold til denne forordning og med vedkommende myndigheter som er opprettet i henhold til denne forordning.

(86) Dersom den leverandøren som opprinnelig brakte aI-systemet i omsetning eller tok det i bruk, på de vilkår som er fastsatt i denne forordning, ikke lenger bør anses som leverandør i henhold til denne forordning, og denne leverandøren ikke uttrykkelig har utelukket at AI-SYSTEMET kan endres til et HØYRISIKO-AII-SYSTEM, bør den tidligere leverandøren likevel samarbeide nært og stille til rådighet de nødvendige opplysninger og gi den tekniske tilgang og annen bistand som med rimelighet kan forventes, og som er nødvendig for å oppfylle forpliktelsene fastsatt i denne forordning, særlig med hensyn til samsvarsvurderingen av høyrisiko-aiI-systemer.

(87) Dersom et høyrisiko-AI-system som er en sikkerhetskomponent i et produkt som faller inn under virkeområdet for Unionens harmoniseringslovgivning basert på den nye rettslige rammen, ikke bringes i omsetning eller tas i bruk uavhengig av produktet, bør produktprodusenten som er definert i denne lovgivningen, oppfylle leverandørens forpliktelser fastsatt i denne forordning, og bør særlig sikre at AI-SYSTEMET som er innebygd i sluttproduktet, er i samsvar med kravene i denne forordning.

(88) langs aI-verdikjeden er det ofte flere parter som leverer aI-systemer, -verktøy og -tjenester, men også komponenter eller prosesser som leverandøren integrerer i AI-SYSTEMET med ulike formål, inkludert modellopplæring, omskolering av modeller, modelltesting og -evaluering, integrering i programvare eller andre aspekter ved modellutvikling. Disse partene har en viktig rolle å spille i verdikjeden overfor leverandøren av høyrisiko-ali-systemet som deres aI-systemer, -verktøy, -tjenester, -komponenter eller -prosesser er integrert i, og bør ved skriftlig avtale gi denne leverandøren nødvendig informasjon, kapasitet, teknisk tilgang og annen bistand basert på det allment anerkjente tekniske nivået, for å gjøre det mulig for leverandøren å oppfylle forpliktelsene fastsatt i denne forordning fullt ut, uten at det går på bekostning av deres egne immaterielle rettigheter eller forretningshemmeligheter.

(89) Tredjeparter som gjør verktøy, tjenester, prosesser eller aI-komponenter, bortsett fra generelle aI-modeller, tilgjengelige for allmennheten, bør ikke pålegges å overholde krav som retter seg mot ansvaret langs aI-verdikjeden, særlig overfor leverandøren som har brukt eller integrert dem, når disse verktøyene, tjenestene, prosessene eller aI-komponentene er gjort tilgjengelige under en fri og åpen kildekodelisens. utviklere av verktøy, tjenester, prosesser eller AI-KOMPONENTER med fri og åpen kildekode som ikke er generelle aI-modeller, bør oppfordres å innføre allment aksepterte dokumentasjonspraksiser, for eksempel modellkort og datablad, som en måte å fremskynde informasjonsdeling langs AI-VERDIKJEDEN på, slik at man kan fremme pålitelige aI-systemer i Unionen.

(90) Kommisjonen kan utvikle og anbefale frivillige standardavtalevilkår mellom leverandører av høyrisiko aI-systemer og tredjeparter som leverer verktøy, tjenester, komponenter eller prosesser som brukes eller integreres i høyrisiko aI-systemer, for å legge til rette for samarbeid langs verdikjeden. Når Kommisjonen utvikler frivillige standardavtalevilkår, bør den også ta hensyn til mulige kontraktskrav som gjelder i bestemte sektorer eller forretningsområder.

(91) Med tanke på AI-SYSTEMENES art og den risiko for sikkerheten og de grunnleggende rettighetene som kan være forbundet med bruken av dem, herunder med hensyn til behovet for å sikre forsvarlig overvåking AV et aI-systems ytelse i en reell situasjon, er det hensiktsmessig å fastsette særlige ansvarsområder for utplasserere. utplasserere bør særlig treffe egnede tekniske og organisatoriske tiltak for å sikre at de bruker høyrisikosystemer I samsvar med bruksanvisningen, og det bør fastsettes visse andre forpliktelser med hensyn til overvåking AV aI-systemenes virkemåte og med hensyn til journalføring, alt etter hva som er relevant. Videre bør utplasseringsforetakene sikre at de personene som har fått i oppdrag å gjennomføre bruksanvisningen og det menneskelige tilsynet som fastsatt i denne forordning, har den nødvendige

kompetanse, særlig et tilstrekkelig nivå AV aI-kunnskaper, opplæring og myndighet til å utføre disse oppgavene på en tilfredsstillende måte. Disse forpliktelsene bør ikke berøre andre forpliktelser som påhviler utplasserere i forbindelse med høyrisikosystemer for kunstig intelligens i henhold til unionsretten eller nasjonal rett.

(92) Denne forordning berører ikke arbeidsgivernes plikt til å informere eller informere og rådføre seg med arbeidstakerne eller deres representanter i henhold til unionsretten eller nasjonal rett og praksis, herunder europaparlaments- og rådsdirektiv 2002/14/EF ([39]), om beslutninger om å ta I bruk eller bruke aI-systemer. Det er fortsatt nødvendig å sikre informasjon til arbeidstakerne og deres representanter om den planlagte innføringen av høyrisikosystemer for KUNSTIG intelligens på arbeidsplassen der vilkårene for slik informasjon eller informasjons- og konsultasjonsforpliktelser i andre rettslige instrumenter ikke er oppfylt. Videre er en slik rett til informasjon underordnet og nødvendig for målet om å beskytte de grunnleggende rettighetene som ligger til grunn for denne forordning. Det bør derfor fastsettes et informasjonskrav med dette formål i denne forordning, uten at det berører arbeidstakernes eksisterende rettigheter.

(93) Selv om risikoer knyttet til AI-SYSTEMER kan skyldes måten slike systemer er utformet på, kan risikoer også oppstå som følge av hvordan slike AI-SYSTEMER brukes. distributører av høyrisiko AI-SYSTEMER spiller derfor en avgjørende rolle når det gjelder å sikre at grunnleggende rettigheter beskyttes, og utfyller leverandørens forpliktelser ved utviklingen av aI-systemet. distributørene har de beste forutsetningene for å forstå hvordan høyrisiko AI-SYSTEMET vil bli brukt konkret, og kan derfor identifisere potensielle betydelige risikoer som ikke ble forutsett i utviklingsfasen, på grunn av mer presis kunnskap om brukskonteksten, personene eller gruppene av personer som sannsynligvis vil bli berørt, herunder sårbare grupper. distributører AV høyrisiko-AI-systemer som er oppført i et vedlegg til denne forordning, spiller også en avgjørende rolle når det gjelder å informere fysiske personer, og bør, når de treffer beslutninger eller bistår med å treffe beslutninger knyttet til fysiske personer, der det er relevant, informere de fysiske personene om at de er gjenstand bruk AV høyrisiko-AI-systemet. Denne informasjonen bør omfatte det tiltenkte formålet og hvilken type beslutninger som tas. Distributøren bør også informere de fysiske personene om deres rett til en forklaring i henhold til denne forordning. Når det gjelder HØYRISIKO-AI-SYSTEMER som brukes til rettshåndhevingsformål, bør denne plikten gjennomføres i samsvar med artikkel 13 i direktiv (EU) 2016/680.

(94) all behandling av biometriske data i forbindelse med bruk AV AI-systemer for biometrisk identifikasjon i forbindelse med rettshåndhevelse må være i samsvar med artikkel 10 i direktiv (EU) 2016/680, som tillater slik behandling bare der det er strengt nødvendig, med forbehold om passende garantier for den registrertes rettigheter og friheter, og der det er tillatt I HENHOLD til unionsretten eller medlemsstatenes nasjonale rett. Når slik bruk er tillatt, må den også respektere prinsippene som er fastsatt i artikkel 4 (1) i direktiv (EU) 2016/680, herunder lovlighet, rettferdighet og åpenhet, formålsbegrensning, nøyaktighet og lagringsbegrensning.

(95) Med forbehold for gjeldende unionsrett, særlig forordning (EU) 2016/679 og direktiv (EU) 2016/680, og med tanke på den inngripende karakteren til systemer for etterfølgende biometrisk identifikasjon, bør bruken av systemer for etterfølgende biometrisk identifikasjon være underlagt sikkerhetstiltak. Systemer for biometrisk identifisering etter fjernkontroll bør alltid brukes på en måte som er forholdsmessig, legitim og strengt nødvendig, og dermed målrettet med hensyn til de personene som skal identifiseres, sted, tidsmessig omfang og basert på et lukket datasett med lovlig innsamlet videomateriale. Biometriske identifikasjonssystemer etter avstandsoppfølging bør uansett ikke brukes i forbindelse med rettshåndhevelse for å føre til vilkårlig overvåking. Vilkårene for biometrisk identifikasjon i etterkant av fjernstyringen bør uansett ikke gi grunnlag for å omgå vilkårene forbudet og de strenge unntakene for biometrisk identifikasjon i sanntid.

(96) For effektivt å sikre at grunnleggende rettigheter beskyttes, bør brukere AV høyrisiko-AI-systemer som er offentligrettslige organer, eller private enheter som yter offentlige tjenester, og brukere visse høyrisiko-AI-systemer som er oppført i et vedlegg til denne forordning, for eksempel bank- eller forsikringsenheter, gjennomføre en konsekvensanalyse av grunnleggende rettigheter før de tar dem i bruk. Tjenester som er viktige for enkeltpersoner, og som er av offentlig karakter, kan også leveres av private enheter. Private enheter som tilbyr slike offentlige tjenester, er knyttet til oppgaver i allmennhetens interesse, for eksempel på områdene utdanning, helsetjenester, sosiale tjenester, bolig og rettspleie. Målet med konsekvensutredningen av grunnleggende rettigheter er at den som skal gjennomføre tiltaket, skal identifisere de spesifikke risikoene for rettighetene til enkeltpersoner eller grupper av enkeltpersoner som sannsynligvis vil bli berørt, og identifisere tiltak som skal iverksettes dersom disse risikoene materialiserer seg. Konsekvensanalysen bør utføres før høyrisikosystemet tas I bruk, og bør oppdateres

(39) Europaparlaments- og rådsdirektiv 2002/14/EF av 11. mars 2002 om fastsettelse av en generell ramme for informasjon og høring av arbeidstakere i Det europeiske fellesskap (EFT L 80 av 23.3.2002, s. 29).

når utrulleren mener at noen av de relevante faktorene har endret seg. Konsekvensvurderingen bør identifisere utbyggerens relevante prosesser der høyrisiko KI-systemet vil bli brukt i tråd med det tiltenkte formålet, og bør omfatte en beskrivelse av tidsperioden og hyppigheten som systemet er ment å bli brukt i, samt av spesifikke kategorier av fysiske personer og grupper som sannsynligvis vil bli berørt i den spesifikke brukssammenhengen. Vurderingen bør også omfatte identifisering av spesifikke skaderisikoer som kan ha innvirkning på de grunnleggende rettighetene til disse personene eller gruppene. Ved utførelsen av denne vurderingen bør utrulleren ta hensyn til informasjon som er relevant for en korrekt vurdering av konsekvensene, herunder, men ikke begrenset til, den informasjonen som leverandøren av høyrisiko KI-systemet har gitt i bruksanvisningen. I lys av de identifiserte risikoene bør distributørene fastsette tiltak som skal treffes dersom disse risikoene materialiserer seg, herunder for eksempel styringsordninger i den spesifikke , for eksempel ordninger for menneskelig tilsyn i henhold til bruksanvisningen eller klagebehandling og klageprosedyrer, ettersom de kan bidra til å redusere risikoene for grunnleggende rettigheter i konkrete brukstilfeller. etter å ha utført denne konsekvensanalysen bør distributøren varsle relevante markedsovervåkningsmyndigheten. For å samle inn relevant informasjon som er nødvendig for å utføre konsekvensanalysen, kan utbyggere AV høyrisikosystemer for kunstig INTELLIGENS, særlig når slike systemer brukes i offentlig sektor, involvere relevante interessenter, herunder representanter for grupper AV personer som sannsynligvis vil bli berørt av systemet, uavhengige eksperter og sivilsamfunnsorganisasjoner, i gjennomføringen av slike konsekvensanalyser og i utformingen av tiltak som skal treffes dersom risikoen materialiserer seg, der dette er hensiktsmessig. European artificial Intelligence Office (aI Office) bør utvikle en mal for et spørreskjema for å gjøre det lettere å etterleve kravene og redusere den administrative byrden for utbyggerne.

(97) Begrepet generelle aI-modeller bør defineres klart og holdes atskilt fra begrepet aI-systemer for å skape rettssikkerhet. Definisjonen bør baseres på de viktigste funksjonelle egenskapene til en generell KI-modell, særlig generaliteten og evnen til å utføre et bredt spekter av forskjellige oppgaver på en kompetent måte. Disse modellene trenes vanligvis opp på store datamengder ved hjelp av ulike metoder, for eksempel selvveiledet, ikke-veiledet eller forsterket læring. Allsidige KI-modeller kan markedsføres på ulike måter, blant annet gjennom biblioteker, programmeringsgrensesnitt for applikasjoner (API-ER), direkte nedlasting eller som fysiske kopier. Disse modellene kan modifiseres ytterligere eller finjusteres til nye modeller. Selv om aI-modeller er viktige komponenter i aI-systemer, utgjør de ikke aI-systemer alene. AI-MODELLER krever tillegg av ytterligere komponenter, som for eksempel et brukergrensesnitt, for å bli AI-SYSTEMER. aI-modeller er vanligvis integrert i og utgjør en del av aI-systemer. Denne forordning fastsetter særlige regler for generelle aI-modeller og for generelle AI-MODELLER som utgjør en systemrisiko, som også bør gjelde når disse modellene er integrert i eller utgjør en del av et AI-SYSTEM. Det bør være underforstått at forpliktelsene for tilbydere av generelle aI-modeller bør gjelde når de generelle aI-modellene er plassert på markedet. Når leverandøren av en generell aI-modell integrerer en egen modell i sitt eget aI-system som gjøres tilgjengelig på markedet eller tas i bruk, bør denne modellen anses for å brakt i omsetning, og forpliktelsene i denne forordning for modeller bør derfor fortsatt gjelde i tillegg til forpliktelsene for aI-systemer. Forpliktelsene som er fastsatt for modeller, bør uansett ikke få anvendelse når en egen modell brukes til rent interne prosesser som ikke er avgjørende for å levere et produkt eller en tjeneste til tredjemann, og fysiske personers rettigheter ikke berøres. Tatt i betraktning deres potensielt betydelig negative virkninger, bør de generelle AI-MODELLENE med systemrisiko alltid være underlagt de relevante forpliktelsene i henhold til denne forordning. Definisjonen bør ikke omfatte KI-modeller som brukes før de bringes i omsetning utelukkende med henblikk på forskning, utvikling og prototyping. Dette berører ikke plikten til å overholde denne forordning når en modell bringes i omsetning etter slike aktiviteter.

(98) Selv om en modells generalitet blant annet også kan bestemmes av antall parametere, bør modeller med minst en milliard parametere og som er trent opp med en stor mengde data ved hjelp av selvovervåking i stor skala, anses å ha en betydelig generalitet og utføre et bredt spekter av oppgaver på en kompetent måte.

(99) Store generative aI-modeller er et typisk eksempel på en generell aI-modell, siden de gir mulighet for fleksibel generering av innhold, for eksempel i form av tekst, lyd, bilder eller video, som lett kan tilpasses et bredt spekter av forskjellige oppgaver.

(100) Når en generell aI-modell er integrert i eller utgjør en del av et aI-system, bør dette systemet betraktes som et generelt AI-SYSTEM når det på grunn av denne integrasjonen kan brukes til en rekke formål. ET generelt AI-SYSTEM kan brukes direkte, eller det kan integreres i andre aI-systemer.

(101) Tilbydere af generelle aI-modeller har en særlig rolle og et særlig ansvar I aI-verdikjeden, ettersom modellene de tilbyr, kan danne grunnlaget for en rekke nedstrømssystemer, som ofte leveres av nedstrømsleverandører som trenger en god forståelse modellene og deres egenskaper, både for å kunne integrere slike modeller i sine produkter og for å oppfylle sine forpliktelser i henhold til dette eller andre regelverk. Det bør derfor fastsettes forholdsmessige tiltak for åpenhet, herunder utarbeidelse og ajourføring av dokumentasjon, samt informasjon om den generelle aI-modellen slik at den kan brukes av nedstrømsleverandører. Den tekniske dokumentasjonen bør utarbeides og holdes oppdatert av leverandøren av den generelle aI-modellen, slik at den på anmodning kan stilles til rådighet for aI-kontoret og de nasjonale vedkommende myndigheter. Minimumssettet av elementer som skal inngå i slik dokumentasjon, bør fastsettes i særskilte vedlegg til denne forordning. Kommisjonen bør gis myndighet til å endre disse vedleggene ved hjelp av delegerte rettsakter i lys av den teknologiske utviklingen.

(102) Programvare og data, herunder modeller, som frigis under en gratis lisens med åpen kildekode som gjør det mulig å dele dem åpent, og der brukerne fritt kan få tilgang til, bruke, endre og videredistribuere dem eller modifiserte versjoner av dem, kan bidra til forskning og innovasjon i markedet og gi betydelige vekstmuligheter for Unionens økonomi. Allsidige KI-modeller som utgis under frie lisenser med åpen kildekode, bør anses å sikre høy grad av gjennomsiktighet og åpenhet dersom deres parametere, herunder vektene, informasjonen om modellarkitekturen og informasjonen om modellbruken gjøres offentlig tilgjengelig. Lisensen bør også anses som fri og åpen kildekode når den tillater brukere å kjøre, kopiere, distribuere, studere, endre og forbedre programvare og data, inkludert modeller, under forutsetning av at den opprinnelige leverandøren av modellen krediteres, og at identiske eller sammenlignbare distribusjonsvilkår respekteres.

(103) Frie aI-komponenter med åpen kildekode dekker programvare og data, inkludert modeller og generelle aI-modeller, verktøy, tjenester eller prosesser i et aI-system. Gratis aI-komponenter med åpen kildekode kan leveres gjennom ulike kanaler, herunder utvikling på åpne repositorier. Ved anvendelsen av denne forordning bør aI-komponenter som leveres mot betaling eller på annen måte omsettes i penger, herunder gjennom av teknisk støtte eller andre tjenester, herunder gjennom en programvareplattform, knyttet til AI-KOMPONENTEN, eller bruk av personopplysninger av andre grunner enn utelukkende for å forbedre programvarens sikkerhet, kompatibilitet eller interoperabilitet, med unntak av transaksjoner mellom mikroforetak, ikke omfattes av unntakene for aI-komponenter med gratis og åpen kildekode. Det å gjøre aI-komponenter tilgjengelige gjennom åpne repositorier bør ikke i seg selv utgjøre en inntektsgenerering.

(104) Tilbydere av generelle aI-modeller som er utgitt under en gratis lisens med åpen kildekode, og hvis parametere, herunder vektene, informasjonen om modellarkitekturen og informasjonen om modellbruken, gjøres offentlig tilgjengelig, bør være omfattet av unntak med hensyn til de åpenhetsrelaterte kravene som stilles til generelle aI-modeller, med mindre de kan anses å utgjøre en systemrisiko, i tilfelle den omstendighet at modellen er åpen og ledsaget av en lisens med åpen kildekode, ikke bør anses være en tilstrekkelig grunn til å utelukke overholdelse av forpliktelsene i henhold til denne forordning. Under alle , gitt at utgivelsen av generelle AI-modeller under en gratis lisens med åpen kildekode ikke nødvendigvis avslører vesentlig informasjon om datasettet som ble brukt til opplæring eller finjustering av modellen, og om hvordan overholdelse av opphavsrettslovgivningen dermed ble sikret, Unntaket for generelle aI-modeller fra overholdelse av de åpenhetsrelaterte kravene bør ikke gjelde plikten til å utarbeide et sammendrag om innholdet som er brukt til modellopplæring, og plikten til å innføre retningslinjer for å overholde Unionens opphavsrettslovgivning, særlig for å identifisere og overholde rettighetsforbeholdet i henhold til artikkel 4 nr. 3 i Europaparlamentets og Rådets direktiv (EU) 2019/790 ([40])

(105) Allsidige AI-modeller, særlig store generative AI-modeller som kan generere tekst, bilder og annet innhold, byr på unike innovasjonsmuligheter, men også på utfordringer for kunstnere, forfattere og andre skapere og måten deres kreative innhold skapes, distribueres, brukes og konsumeres på. Utvikling og opplæring av slike modeller krever tilgang til enorme mengder tekst, bilder, videoer og andre data. Teknikker for tekst- og datautvinning kan brukes i utstrakt grad i denne sammenhengen for å hente ut og analysere slikt innhold, som kan være beskyttet av opphavsrett og beslektede rettigheter. all bruk av opphavsrettsbeskyttet innhold krever tillatelse fra den berørte rettighetshaveren, med mindre det gjelder relevante unntak og begrensninger i opphavsretten. direktiv (EU) 2019/790 innførte unntak og begrensninger som tillater reproduksjon og utdrag av verk eller annet materiale, med henblikk på tekst- og datautvinning.

(40) Europaparlaments- og rådsdirektiv (EU) 2019/790 av 17. april 2019 om opphavsrett og beslektede rettigheter i det digitale indre marked og om endring av direktiv 96/9/EF og 2001/29/EF (EUT L 130 av 17.5.2019, s. 92).

utvinning, på visse vilkår. I henhold til disse reglene kan rettighetshavere velge å reservere sine rettigheter over sine verk eller andre frembringelser for å forhindre tekst- og datautvinning, med mindre dette gjøres i forbindelse med vitenskapelig forskning. Der retten til å reservere seg er uttrykkelig forbeholdt PÅ EN hensiktsmessig måte, må tilbydere av generelle AI-modeller innhente tillatelse fra rettighetshaverne dersom de ønsker å utføre tekst- og datautvinning i slike verk.

(106) Tilbydere som plasserer allsidige AI-MODELLER på unionsmarkedet, bør sikre overholdelse av de relevante forpliktelsene i denne forordning. For dette formål bør tilbydere av generelle aI-modeller innføre retningslinjer for overholde unionsretten om opphavsrett og nærstående rettigheter, særlig for å identifisere og overholde rettighetshavernes forbehold om rettigheter i henhold til artikkel 4 nr. 3 i direktiv (EU) 2019/790. Enhver tilbyder som plasserer en generell aI-modell på unionsmarkedet, bør overholde denne forpliktelsen, uavhengig av I hvilken jurisdiksjon de opphavsrettsrelevante handlingene som ligger til grunn for opplæringen disse generelle aI-modellene, finner sted. Dette er nødvendig for å sikre like vilkår for alle tilbydere av allsidige aI-modeller, der ingen tilbyder bør kunne oppnå et konkurransefortrinn på unionsmarkedet ved å anvende lavere opphavsrettslige standarder enn dem som gjelder i Unionen.

(107) For å øke åpenheten om dataene som brukes i forhåndstreningen og treningen av generelle AI-MODELLER, herunder tekst og data som er beskyttet av opphavsrettslovgivningen, er det tilstrekkelig at tilbydere av slike modeller utarbeider og offentliggjør et tilstrekkelig detaljert sammendrag av innholdet som brukes til å trene den generelle aI-modellen. Selv om det tas behørig hensyn til behovet for å beskytte forretningshemmeligheter og konfidensiell forretningsinformasjon, bør dette sammendraget være generelt omfattende i stedet for teknisk detaljert for å gjøre det lettere for parter med legitime interesser, herunder opphavsrettsinnehavere, å utøve og håndheve sine rettigheter i henhold til , for eksempel ved å liste opp de viktigste datasamlingene eller datasettene som inngikk i treningen av modellen, for eksempel store private eller offentlige databaser eller dataarkiver, og ved å gi en fortellende forklaring om andre datakilder som er brukt. Det er hensiktsmessig at AI-kontoret tilbyr en mal for sammendraget, som bør være enkel og effektiv, og som gjør det mulig for leverandøren å det påkrevde sammendraget i narrativ form.

(108) Når det gjelder forpliktelsene som pålegges tilbydere av allmenne AI-modeller til å innføre retningslinjer for å overholde Unionens opphavsrettslovgivning og offentliggjøre et sammendrag av innholdet som brukes til opplæringen, bør AI-kontoret overvåke om tilbyderen har oppfylt disse forpliktelsene uten å verifisere eller foreta en vurdering av opplæringsdataene arbeid for arbeid med hensyn til overholdelse av opphavsretten. Denne forordningen påvirker ikke håndhevelsen av opphavsrettslige regler i henhold til unionsretten.

(109) Overholdelsen AV forpliktelsene som gjelder for tilbydere av allmenne KI-modeller, bør stå I forhold til og STÅ I et rimelig forhold til typen , med unntak av behovet for overholdelse for personer som utvikler eller bruker modeller for ikke-profesjonelle eller vitenskapelige forskningsformål, som likevel bør oppfordres til frivillig å overholde disse kravene. Uten at det berører Unionens opphavsrettslovgivning, bør overholdelsen av disse forpliktelsene ta behørig hensyn til tilbyderens størrelse og tillate forenklede måter å overholde kravene på for små og mellomstore bedrifter, herunder nyetablerte foretak, som ikke bør medføre uforholdsmessig store kostnader og ikke motvirke bruken av slike modeller. Dersom en modell endres eller finjusteres, bør forpliktelsene for tilbydere av generelle aI-modeller begrenses til denne endringen eller finjusteringen, for eksempel ved å utfylle den allerede eksisterende tekniske dokumentasjonen med informasjon om endringene, herunder nye opplæringsdatakilder, som et middel til å oppfylle verdikjedeforpliktelsene fastsatt i denne forordning.

(110) Allmenne KI-modeller kan utgjøre systemiske risikoer som omfatter, men ikke er begrenset til, faktiske eller rimelig forutsigbare negative effekter i forbindelse med større ulykker, forstyrrelser i kritiske sektorer og alvorlige konsekvenser for folkehelsen og sikkerheten, faktiske eller rimelig forutsigbare negative effekter på demokratiske prosesser, offentlig og økonomisk sikkerhet, spredning ulovlig, falskt eller diskriminerende innhold. Systemrisiko bør forstås slik at den øker med modellens kapasitet og rekkevidde, kan oppstå gjennom hele modellens livssyklus og påvirkes av forhold som misbruk, modellens pålitelighet, modellens rettferdighet og modellsikkerhet, modellens grad av autonomi, modellens

modellen, tilgangen til verktøy, nye eller kombinerte modaliteter, frigjørings- og distribusjonsstrategier, potensialet for å fjerne beskyttelsestiltak og andre faktorer. Internasjonale tilnærminger har så langt identifisert behovet for å ta hensyn til risikoer som følge av potensielt tilsiktet misbruk eller utilsiktede kontrollproblemer knyttet til tilpasning til menneskelige intensjoner; kjemiske, biologiske, radiologiske og kjernefysiske risikoer, for eksempel hvordan inngangsbarrierer kan senkes, inkludert for våpenutvikling, design, anskaffelse eller bruk; offensive cyberkapabiliteter, for eksempel hvordan sårbarhetsoppdagelse, utnyttelse eller operativ bruk kan muliggjøres; effektene av interaksjon og verktøybruk, inkludert for eksempel kapasiteten til å kontrollere fysiske systemer og forstyrre kritisk infrastruktur; risiko for at modeller kan lage kopier seg selv eller "selvreplikere" eller lære opp andre modeller; hvordan modeller kan gi opphav til skadelige fordommer og diskriminering med risiko for enkeltpersoner, lokalsamfunn eller samfunn; tilrettelegging for desinformasjon eller skade på personvernet med trusler mot demokratiske verdier og menneskerettigheter; risiko for at en bestemt hendelse kan føre til en kjedereaksjon med betydelige negative effekter som kan påvirke opptil en hel by, en hel domeneaktivitet eller et helt samfunn.

(111) Det bør fastsettes en metode for klassifisering av generelle aI-modeller som generelle aI-modeller med systemrisiko. Ettersom systemrisiko er et resultat av særlig høy kapasitet, bør en generell aI-modell anses å utgjøre en systemrisiko dersom den har kapasitet med stor innvirkning, evaluert på grunnlag av egnede tekniske verktøy og metoder, eller betydelig innvirkning på det indre marked på grunn av sin rekkevidde. Med stor gjennomslagskraft i generelle AI-MODELLER menes kapasiteter som tilsvarer eller overgår kapasitetene som er registrert i de mest avanserte generelle aI-modellene. I henhold til det aktuelle tekniske på tidspunktet for denne forordnings ikrafttredelse er den kumulative beregningsmengden som brukes til opplæring av den generelle aI-modellen, målt I flyttalloperasjoner, en av de relevante tilnærmingene modellkapasiteter. Den kumulative beregningsmengden som brukes til opplæring, omfatter beregningene som brukes på tvers av aktiviteter og metoder er ment å forbedre modellens kapasitet før utplassering, for eksempel forhåndstrening, generering av syntetiske data og finjustering. Derfor bør det settes en innledende terskelverdi for flyttallsoperasjoner, som, hvis den oppfylles av en generell , fører til en antakelse om at modellen ER EN GENERELL aI-modell med systemrisiko. Denne terskelen bør justeres over tid for å gjenspeile teknologiske og industrielle endringer, for eksempel algoritmiske forbedringer eller økt maskinvareeffektivitet, og bør suppleres med referanseverdier og indikatorer for modellkapasitet. For å bidra til dette bør AI Office samarbeide med forskningsmiljøer, bransjen, sivilsamfunnet og andre eksperter. Terskelverdier, samt verktøy og referanseverdier for vurdering av kapasiteter med stor innvirkning, bør være sterke indikatorer for generalitet, kapasitet og tilhørende systemrisiko for generelle aI-modeller, og kan ta hensyn til hvordan modellen vil bli markedsført eller hvor mange brukere den kan påvirke. For å utfylle dette systemet bør det være mulig for Kommisjonen å treffe individuelle beslutninger om å utpeke en generell AI-MODELL som en generell AI-MODELL med systemrisiko dersom det viser seg at en slik modell har egenskaper eller en innvirkning som tilsvarer dem som fanges opp av den fastsatte terskelen. Denne beslutningen bør treffes på grunnlag av en samlet vurdering av kriteriene for utpeking AV en generell AI-MODELL med systemrisiko som er i et vedlegg til denne forordning, f.eks. kvaliteten eller størrelsen på opplæringsdatasettet, antall forretnings- og sluttbrukere, dens inndata- og utdatamodaliteter, dens grad av autonomi og skalerbarhet eller verktøyene den har tilgang til. Etter en begrunnet anmodning fra en tilbyder hvis modell har blitt utpekt som en generell AI-MODELL med systemrisiko, bør Kommisjonen ta hensyn til anmodningen og kan beslutte å revurdere hvorvidt DEN GENERELLE aI-modellen fortsatt kan anses å utgjøre en systemrisiko.

(112) Det er også nødvendig å klargjøre en prosedyre for klassifisering av en generell aI-modell med systemrisiko. EN generell aI-modell som oppfyller den gjeldende terskelen for high impact capabilities, bør presumeres å være en generell aI-modell med systemrisiko. Tilbyderen bør varsle aI-kontoret senest to uker etter at kravene er oppfylt eller det blir kjent at en generell AI-MODELL vil oppfylle kravene som fører til presumpsjon. Dette er særlig relevant i forhold til terskelen for flyttallsoperasjoner fordi opplæring av generelle aI-modeller krever betydelig planlegging som inkluderer forhåndsallokering av beregningsressurser, og leverandører av generelle AI-MODELLER er derfor i stand til å vite om modellen deres vil oppfylle terskelen før opplæringen er fullført. I forbindelse med denne meldingen bør leverandøren kunne påvise at en generell aI-modell, på grunn av sine spesifikke egenskaper, unntaksvis ikke utgjør en systemrisiko, og at den dermed ikke bør klassifiseres som en generell AI-MODELL med systemrisiko. Denne informasjonen er verdifull for aI-kontoret for å forutse markedsføringen av generelle aI-modeller med systemrisiko, og leverandørene kan begynne å samarbeide med aI-kontoret på et tidlig tidspunkt. Denne informasjonen er spesielt

viktig med hensyn til generelle aI-modeller som planlegges utgitt som åpen kildekode, ettersom det etter utgivelsen av åpen kildekode-modellen kan være vanskeligere å gjennomføre nødvendige tiltak for å sikre samsvar med forpliktelsene i henhold til denne forordningen.

(113) Dersom Kommisjonen blir oppmerksom på at en generell KI-modell oppfyller kravene til å klassifiseres som en generell KI-modell med systemrisiko, noe som tidligere enten ikke har vært kjent eller som den relevante leverandøren har varslet Kommisjonen om, Kommisjonen ha myndighet til å utpeke den som en slik modell. ET system med kvalifiserte varsler bør sikre at KI-kontoret blir gjort oppmerksom på generelle KI-modeller som muligens bør klassifiseres som generelle KI-MODELLER med systemrisiko, I tillegg til KI-KONTORETS overvåkingsaktiviteter, av det vitenskapelige panelet.

(114) Tilbydere av generelle aI-modeller som utgjør en systemrisiko, bør i tillegg til forpliktelsene som gjelder for tilbydere av generelle aI-modeller, være underlagt forpliktelser som tar sikte på å identifisere og avbøte disse risikoene og sikre et tilstrekkelig nivå av cybersikkerhetsbeskyttelse, uavhengig av om den leveres som en frittstående modell eller er innebygd I ET aI-system eller et produkt. For å oppnå disse målene bør denne forordning kreve at tilbydere utfører de nødvendige modellevalueringene, særlig før de bringes i omsetning for første gang, herunder at de gjennomfører og dokumenterer kontradiktorisk testing av modeller, eventuelt også ved hjelp av intern eller uavhengig ekstern testing. I tillegg bør tilbydere av generelle aI-modeller med fortløpende vurdere og redusere systemrisikoen, blant annet ved å innføre retningslinjer for risikohåndtering, for eksempel ansvarlighets- og styringsprosesser, gjennomføre overvåking etter markedsføring, treffe egnede tiltak gjennom hele modellens livssyklus og samarbeide med relevante aktører I aI-verdikjeden.

(115) Leverandører av generelle AI-MODELLER med bør vurdere og redusere mulige systemrisikoer. Dersom utviklingen eller bruken av en generell aI-modell, til tross for innsatsen for å identifisere og forebygge risikoer knyttet en generell aI-modell som kan utgjøre en systemrisiko, forårsaker en alvorlig hendelse, bør leverandøren av den generelle aI-modellen uten unødig opphold holde oversikt over hendelsen og rapportere all relevant informasjon og eventuelle korrigerende tiltak til Kommisjonen og nasjonale vedkommende myndigheter. Videre bør tilbydere sikre et tilstrekkelig nivå av cybersikkerhetsbeskyttelse for modellen og dens fysiske infrastruktur, hvis det er relevant, gjennom hele modellens livssyklus. Cybersikkerhetsbeskyttelse knyttet til systemrisikoer forbundet med ondsinnet bruk eller angrep bør ta behørig hensyn til utilsiktet modelllekkasje, uautoriserte utgivelser, omgåelse av sikkerhetstiltak og forsvar mot cyberangrep, uautorisert tilgang eller tyveri av modeller. Denne beskyttelsen kan gjøres lettere ved å sikre modellvekter, algoritmer, servere og datasett, for eksempel gjennom operasjonelle sikkerhetstiltak for , spesifikke retningslinjer for cybersikkerhet, adekvate tekniske og etablerte løsninger og cyber- og fysiske tilgangskontroller som er tilpasset de relevante omstendighetene og risikoene som er involvert.

(116) aI-kontoret bør oppmuntre til og legge til rette for , gjennomgang og tilpasning av retningslinjer for god praksis, der det tas hensyn til internasjonale tilnærminger. alle leverandører av generelle aI-modeller kan inviteres til å delta. For å sikre at retningslinjene gjenspeiler det nyeste innen feltet og tar behørig hensyn til ET mangfold av perspektiver, bør aI-kontoret samarbeide med relevante nasjonale kompetente myndigheter, og kan, der det er hensiktsmessig, rådføre seg med sivilsamfunnsorganisasjoner andre relevante interessenter og eksperter, inkludert vitenskapspanelet, i forbindelse med utarbeidelsen av slike retningslinjer. Retningslinjene bør omfatte forpliktelser for tilbydere av generelle aI-modeller og av generelle aI-modeller som utgjør en systemrisiko. Når det gjelder systemrisikoer, bør i tillegg bidra til å etablere en risikotaksonomi for typen og arten av systemrisikoer på unionsnivå, herunder kildene til disse. Retningslinjene bør også fokusere på spesifikk risikovurdering og risikoreduserende tiltak.

(117) Praksisreglene bør utgjøre et sentralt verktøy for korrekt overholdelse av forpliktelsene fastsatt i denne forordning for tilbydere av allsidige AI-modeller. Tilbyderne bør kunne basere seg på retningslinjene for god praksis for å påvise at de oppfyller forpliktelsene. Kommisjonen kan ved hjelp av gjennomføringsrettsakter beslutte å godkjenne en kodeks for god praksis og gi den generell gyldighet i Unionen, eller alternativt fastsette felles regler for gjennomføringen av de relevante forpliktelsene, dersom en kodeks for god praksis ikke kan ferdigstilles eller ikke anses som tilstrekkelig av aI-kontoret på det tidspunktet denne forordning får anvendelse. Når en harmonisert standard er

publisert og vurdert som egnet til å dekke de relevante forpliktelsene AV aI-kontoret, bør samsvar med en europeisk harmonisert standard gi leverandørene en presumsjon om samsvar. Tilbydere av generelle aI-modeller bør dessuten kunne demonstrere samsvar ved hjelp av alternative, metoder, dersom det ikke finnes etiske retningslinjer eller harmoniserte standarder, eller dersom de velger å ikke basere seg på disse.

(118) Denne forordning regulerer KI-systemer og KI-modeller ved å innføre visse krav og forpliktelser for relevante markedsaktører som bringer dem i omsetning, tar dem i bruk eller bruker dem i Unionen, og utfyller dermed forpliktelsene for tilbydere av formidlingstjenester som bygger slike systemer modeller inn i sine tjenester, som er regulert I forordning (EU) 2022/2065. I den grad slike systemer eller modeller er integrert i utpekte svært store nettbaserte plattformer eller svært store nettbaserte søkemotorer, er de underlagt rammen for risikohåndtering fastsatt i forordning (EU) 2022/2065. Følgelig bør de tilsvarende forpliktelsene i denne forordning antas å være oppfylt, med mindre det oppstår og identifiseres betydelig systemrisiko som ikke omfattes av forordning (EU) 2022/2065, i slike modeller. Innenfor dette rammeverket er tilbydere av svært store nettbaserte plattformer og svært store nettbaserte søkemotorer forpliktet til å vurdere potensielle systemrisikoer som følger av utformingen, funksjonen og bruken av tjenestene deres, herunder hvordan utformingen av algoritmesystemer som brukes i tjenesten, kan bidra til slike risikoer, samt systemrisikoer som følger av potensielt misbruk. Disse tilbyderne er også forpliktet til å treffe egnede risikoreduserende tiltak i samsvar med grunnleggende rettigheter.

(119) Med tanke på den raske innovasjonstakten og den teknologiske utviklingen av digitale tjenester som omfattes av ulike unionsrettslige instrumenter, særlig med tanke på mottakernes bruk og oppfatning, kan aI-systemene som omfattes av denne forordning, leveres som formidlingstjenester eller deler av formidlingstjenester i henhold forordning (EU) 2022/2065, som bør tolkes på en teknologinøytral måte. For eksempel kan brukes til å tilby søkemotorer på nettet, særlig i den grad ET aI-system, for eksempel en nettbasert chatbot, utfører søk på i prinsippet alle nettsteder, deretter innlemmer resultatene i sin eksisterende kunnskap og bruker den oppdaterte kunnskapen til å generere ett enkelt resultat som kombinerer ulike informasjonskilder.

(120) Videre er forpliktelsene som i denne forordning pålegges tilbydere og brukere av visse AI-systemer for å gjøre det mulig å oppdage og avsløre at resultatene fra disse systemene er kunstig generert eller manipulert, særlig relevante for å legge til rette for en effektiv gjennomføring av forordning (EU) 2022/2065. Dette gjelder særlig forpliktelsene for leverandører av svært store nettplattformer eller svært store søkemotorer på nettet til å identifisere og avbøte systemrisikoer som kan oppstå som følge av spredning av innhold som er kunstig generert eller manipulert, særlig risikoen for faktiske eller forutsigbare negative virkninger på demokratiske prosesser, og valgprosesser, herunder gjennom desinformasjon.

(121) Standardisering bør spille en nøkkelrolle for å tilby tekniske løsninger til tilbydere for å sikre samsvar med denne forordning, i tråd med det aktuelle tekniske nivået, for å fremme innovasjon samt konkurranseevne og vekst i det indre marked. Overholdelse av harmoniserte standarder som definert i artikkel 2 . 1 bokstav c) i europaparlaments- og rådsforordning (EU) nr. 1025/2012 ((41)), som normalt forventes å gjenspeile det aktuelle tekniske nivå, bør være et middel for tilbydere til å påvise samsvar med kravene i denne forordning. Det bør derfor oppmuntres til en balansert interesserepresentasjon som involverer alle relevante interessenter i utviklingen av standarder, særlig små og mellomstore bedrifter, forbrukerorganisasjoner og interessenter på miljø- og samfunnsområdet i samsvar med artikkel 5 og 6 i forordning (EU) nr. 1025/2012. For å gjøre det lettere å oppfylle kravene bør standardiseringsanmodningene utstedes av Kommisjonen uten unødig forsinkelse. Når Kommisjonen utarbeider standardiseringsanmodningen, bør den rådføre seg med det rådgivende forumet og styret for å innhente relevant ekspertise. Dersom det ikke finnes relevante henvisninger til harmoniserte standarder, bør Kommisjonen imidlertid, ved hjelp av gjennomføringsrettsakter og etter samråd med det rådgivende forumet, kunne fastsette felles spesifikasjoner visse krav i henhold til denne forordning. Den felles spesifikasjonen bør være en unntaksløsning for å lette leverandørens plikt til å oppfylle kravene i denne forordning når anmodningen om standardisering ikke er godtatt av noen av de europeiske standardiseringsorganisasjonene, eller når de relevante harmoniserte standardene ikke i tilstrekkelig grad ivaretar hensynet til grunnleggende rettigheter, eller når de harmoniserte standardene ikke er i samsvar med anmodningen, eller når det er forsinkelser i vedtakelsen av en egnet harmonisert standard. Dersom en slik forsinkelse i vedtakelsen av en harmonisert standard skyldes standardens tekniske kompleksitet, bør dette

(41) Europaparlaments- og rådsforordning (EU) nr. 1025/2012 av 25. oktober 2012 om europeisk standardisering, om endring av rådsdirektiv 89/686/EØF og 93/15/EØF og av europaparlaments- og rådsdirektiv 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 oppheving av rådsbeslutning 87/95/EØF og europaparlaments- og rådsbeslutning nr. 1673/2006/EF (EUT L 316 av 14.11.2012, p. 12).

vurderes av Kommisjonen før den vurderer å etablere felles spesifikasjoner. Ved utviklingen av felles spesifikasjoner oppfordres Kommisjonen til å samarbeide med internasjonale partnere og internasjonale standardiseringsorganer.

(122) Uten at det berører bruken av harmoniserte standarder og felles spesifikasjoner, bør det, uten at det berører bruken harmoniserte standarder og felles spesifikasjoner, antas at leverandører av et HØYRISIKO-AI-SYSTEM som har fått opplæring og er testet på data som gjenspeiler de spesifikke geografiske, atferdsmessige, kontekstuelle eller funksjonelle omgivelsene som AI-SYSTEMET er ment å brukes i, oppfyller det relevante tiltaket som er fastsatt i henhold til kravet om dataforvaltning i denne forordning. Uten AT det berører kravene til robusthet og nøyaktighet i denne forordning, bør høyrisiko-AI-systemer som er sertifisert eller som det er utstedt en samsvarserklæring for i henhold til en nettsikkerhetsordning i henhold til nevnte forordning, og hvis henvisninger er offentliggjort i *Den europeiske unions* tidende, i samsvar med artikkel 54 nr. 3 i forordning (*EU)* 2019/881, forutsettes å oppfylle nettsikkerhetskravet i denne forordning i den utstrekning nettsikkerhetssertifikatet eller samsvarserklæringen eller deler av disse dekker nettsikkerhetskravet i denne forordning, uten at det berører kravene til robusthet og nøyaktighet fastsatt I denne forordning. Dette berører ikke cybersikkerhetsordningens frivillige karakter.

(123) For å sikre en høy grad av pålitelighet for høyrisikosystemer bør disse systemene en samsvarsvurdering de bringes i omsetning eller tas i bruk.

(124) For å minimere byrden for de driftsansvarlige og unngå mulig dobbeltarbeid er det hensiktsmessig at for HØYRISIKO-AI-SYSTEMER knyttet til produkter som omfattes av eksisterende EU-harmoniseringsregelverk basert på den nye rettslige rammen, bør disse AI-systemenes samsvar med kravene i denne forordning vurderes som en del av samsvarsvurderingen som allerede er fastsatt i nevnte regelverk. Anvendelsen av kravene i denne forordning bør derfor ikke påvirke den spesifikke logikken, metodikken eller den generelle strukturen for samsvarsvurderingen i henhold til den relevante harmoniseringslovgivningen i Unionen.

(125) På grunn av kompleksiteten ved høyrisiko-AI-systemer og risikoene som er forbundet med dem, er det viktig å utvikle en egnet framgangsmåte for samsvarsvurdering for høyrisiko-AI-systemer som involverer meldte organer, såkalt tredjeparts samsvarsvurdering. Med tanke på den nåværende erfaringen som profesjonelle sertifiseringsorganer før markedsføring har på produktsikkerhetsområdet, og de ulike typene risikoer som er involvert, er det imidlertid hensiktsmessig å begrense, i det minste i en innledende fase av anvendelsen av denne forordning, virkeområdet for tredjeparts samsvarsvurdering for andre høyrisiko-AI-systemer enn dem som er knyttet til produkter. Samsvarsvurderingen av slike systemer bør derfor som hovedregel utføres av leverandøren på eget ansvar, med det eneste unntaket for KI-SYSTEMER som er beregnet på å brukes til biometri.

(126) For å kunne utføre samsvarsvurderinger utført av tredjepart når det kreves, bør meldte organer meldes i henhold til denne forordning av de nasjonale vedkommende myndigheter, forutsatt at de oppfyller et sett med krav, særlig om uavhengighet, kompetanse, fravær av interessekonflikter og egnede krav til IKT-sikkerhet. Melding om disse organene bør sendes av nasjonale vedkommende myndigheter til Kommisjonen og de andre medlemsstatene ved hjelp av det elektroniske meldingsverktøyet som er utviklet og forvaltes av Kommisjonen i henhold til artikkel R23 i vedlegg I til beslutning nr. 768/2008/EF.

(127) I tråd med Unionens forpliktelser i henhold til Verdens handelsorganisasjons avtale om tekniske handelshindre er det hensiktsmessig å legge til rette for gjensidig anerkjennelse av samsvarsvurderingsresultater som er framlagt av kompetente samsvarsvurderingsorganer, uavhengig av hvilket territorium de er etablert på, forutsatt at disse samsvarsvurderingsorganene som er etablert i henhold til lovgivningen i en tredjestat, oppfyller de gjeldende kravene i denne forordning, og Unionen har inngått en avtale om dette. denne sammenheng bør Kommisjonen aktivt undersøke mulige internasjonale instrumenter for dette formål og særlig arbeide for å inngå avtaler om gjensidig godkjenning med tredjestater.

(128) I tråd med det alminnelig etablerte begrepet vesentlig endring for produkter som er regulert av Unionens harmoniseringsregelverk, er det hensiktsmessig at når det skjer en endring som kan påvirke et høyrisiko-AI-systems samsvar med denne forordning (f.eks. endring av operativsystem eller programvarearkitektur), eller når det tiltenkte formålet med systemet endres, bør dette AI-SYSTEMET anses som et nytt AI-system som bør gjennomgå en ny samsvarsvurdering. Endringer i algoritmen og ytelsen til KI-systemer som fortsetter å "lære" etter at de er brakt i omsetning eller tatt i bruk, dvs. som automatisk tilpasser hvordan funksjoner utføres, bør imidlertid ikke utgjøre en vesentlig endring, forutsatt at disse endringene er forhåndsbestemt av leverandøren og vurdert på tidspunktet for samsvarsvurderingen.

(129) Høyrisiko aI-systemer skal være CE-merket for å vise at de er i samsvar med denne forordningen, slik at de kan bevege seg fritt i det indre marked. For høyrisiko AI-SYSTEMER som er innebygd i et produkt, bør det påføres en fysisk CE-merking, som kan suppleres med en digital CE-merking. For HØYRISIKO-AI-SYSTEMER som kun leveres digitalt, bør det brukes en digital CE-merking. Medlemsstatene bør ikke skape ubegrunnede hindringer for omsetning eller ibruktaking AV HØyrisiko-AI-systemer som oppfyller kravene fastsatt i denne forordning, og som er CE-merket.

(130) Under visse forhold kan rask tilgang til innovative teknologier være avgjørende for menneskers helse og sikkerhet, for miljøvern og klimaendringer og for samfunnet som helhet. Det er derfor hensiktsmessig at markedstilsynsmyndighetene i unntakstilfeller, av hensyn til offentlig sikkerhet eller vern av fysiske personers liv og helse, miljøvern og vern av viktige industri- og infrastrukturanlegg, kan gi tillatelse til å bringe I OMSETNING ELLER TA I bruk KI-systemer som ikke har gjennomgått en samsvarsvurdering. I behørig begrunnede situasjoner, som fastsatt i denne forordning, kan eller sivilbeskyttelsesmyndigheter ta i bruk et spesifikt høyrisikosystem uten tillatelse fra markedstilsynsmyndigheten, forutsatt at det anmodes om en slik tillatelse under eller etter bruken uten unødig forsinkelse.

(131) For å lette Kommisjonens og medlemsstatenes arbeid på AI-OMRÅDET og for å øke åpenheten overfor allmennheten bør leverandører av andre høyrisiko-ai-systemer enn dem som er knyttet til produkter som omfattes av relevant eksisterende , samt leverandører som anser at et som er oppført i høyrisikobruktilfellene i et vedlegg til denne forordning, ikke utgjør en høyrisiko på grunnlag av ET unntak, å registrere seg selv og opplysninger om sitt AI-SYSTEM i en EU-database som skal opprettes og forvaltes av Kommisjonen. Før de tar i bruk et AI-SYSTEM som er oppført i høyrisikobrukstilfellene i et vedlegg til denne forordning, bør brukere av aI-systemer med høy risiko som er offentlige myndigheter, byråer eller organer, registrere seg i en slik database og velge det systemet de planlegger å bruke. Andre utbyggere bør ha rett til å gjøre dette frivillig. Denne delen av EU-databasen bør være offentlig tilgjengelig og , og informasjonen bør være lett å navigere i, forståelig og maskinlesbar. EU-databasen bør også være brukervennlig, for eksempel ved å tilby søkefunksjoner, blant annet ved hjelp av nøkkelord, slik at allmennheten kan finne relevant informasjon som skal sendes inn ved registrering av HØYRISIKO-AI-SYSTEMER og om bruksområdet for HØYRISIKO-AI-SYSTEMER, som er fastsatt i et vedlegg til denne forordning, som høyrisiko-AI-systemene tilsvarer. enhver vesentlig endring av HØYRISIKO-AI-SYSTEMER bør også registreres i EU-databasen. For høyrisiko AI-SYSTEMER på rettshåndhevelse, migrasjon, asyl og grensekontrollforvaltning bør registreringsforpliktelsene oppfylles i en sikker, ikke-offentlig del av EU-databasen. tilgangen til den sikre, ikke-offentlige delen bør være strengt begrenset til Kommisjonen og til markedstilsynsmyndighetene med hensyn til deres nasjonale del denne databasen. Høyrisiko-AI-systemer på området kritisk infrastruktur bør kun registreres på nasjonalt nivå. Kommisjonen bør være behandlingsansvarlig for EU-databasen, i samsvar med forordning (EU) 2018/1725. For å sikre at EU-databasen fungerer fullt ut når den tas i bruk, bør prosedyren for etablering av databasen omfatte utarbeidelse av funksjonelle spesifikasjoner av Kommisjonen og en uavhengig revisjonsrapport. Kommisjonen bør ta hensyn til cybersikkerhetsrisikoer når den utfører sine oppgaver som behandlingsansvarlig for EU-databasen. For å maksimere tilgjengeligheten og bruken av EU-databasen for allmennheten bør EU-databasen, herunder informasjonen som gjøres tilgjengelig gjennom den, oppfylle kravene i direktiv (EU) 2019/882.

(132) Visse AI-SYSTEMER som er beregnet på å samhandle med fysiske personer eller generere innhold, kan utgjøre en særlig risiko for etterligning eller bedrageri, uavhengig av om de kvalifiserer som høyrisikosystemer eller ikke. Under visse omstendigheter bør bruken av disse systemene derfor være underlagt særlige åpenhetsforpliktelser, uten at det berører kravene og forpliktelsene for høyrisikosystemer for KUNSTIG INTELLIGENS, og med målrettede unntak for å ta hensyn til rettshåndhevingsorganenes særlige behov. Fysiske personer bør særlig underrettes om at de samhandler med ET AI-SYSTEM, med mindre dette er åpenbart for en fysisk person som er rimelig velinformert, oppmerksom og veloverveid, omstendighetene og brukssammenhengen tatt i betraktning. Ved gjennomføringen av denne forpliktelsen bør det tas hensyn til særtrekkene ved fysiske personer som tilhører sårbare grupper på grunn av alder eller nedsatt funksjonsevne, I DEN grad KI-systemet også er ment å samhandle med disse gruppene. Videre bør fysiske personer varsles når de eksponeres FOR aI-systemer som, ved å behandle deres biometriske data, kan identifisere eller utlede disse personenes følelser eller intensjoner eller tilordne dem til bestemte kategorier. Slike spesifikke kategorier kan være knyttet til aspekter som kjønn, alder, hårfarge, øyenfarge, tatoveringer, personlige egenskaper, etnisk opprinnelse, personlige preferanser og interesser. Slik informasjon og slike varsler bør gis i formater som er tilgjengelige for personer med nedsatt funksjonsevne.

(133) en rekke KI-systemer kan generere store mengder syntetisk innhold som det blir stadig vanskeligere for mennesker å skille fra menneskeskapt og autentisk innhold. Den store tilgjengeligheten og den økende kapasiteten til disse systemene har en betydelig innvirkning på integriteten og tilliten til informasjonsøkosystemet, og skaper nye risikoer for feilinformasjon og manipulasjon i stor skala, svindel, etterligning og forbrukerbedrag. I lys av disse konsekvensene, den raske teknologiske utviklingen og behovet for nye metoder og teknikker for å spore informasjonens opprinnelse, er det hensiktsmessig å kreve at leverandører av slike systemer bygger inn tekniske løsninger som muliggjør merking i et maskinlesbart format og påvisning AV AT utdataene har blitt generert eller manipulert AV ET KI-system og ikke av ET menneske. Slike teknikker og metoder bør være tilstrekkelig pålitelige, interoperable, effektive og robuste så langt det er teknisk mulig, idet det tas hensyn til tilgjengelige teknikker eller en kombinasjon av slike teknikker, f.eks. vannmerker, metadataidentifikasjoner, kryptografiske metoder for å bevise innholdets opprinnelse og autentisitet, loggføringsmetoder, fingeravtrykk eller andre teknikker, alt etter hva som er hensiktsmessig. Ved gjennomføringen av denne forpliktelsen bør tilbyderne også ta hensyn til særtrekkene og begrensningene ved de ulike innholdstypene og den relevante teknologiske og utviklingen på området, slik den gjenspeiles i det allment anerkjente tekniske utviklingsnivået. Slike teknikker og metoder kan gjennomføres på nivået for aI-systemet eller på nivået for aI-modellen, herunder generelle AI-MODELLER som genererer innhold, og dermed gjøre det lettere for nedstrømsleverandøren av aI-systemet å oppfylle denne forpliktelsen. For å være forholdsmessig er det hensiktsmessig å se for seg at denne merkeplikten ikke bør omfatte aI-systemer som primært utfører en hjelpefunksjon for standardredigering, eller som ikke i vesentlig grad endrer inngangsdataene som leveres av utrulleren eller semantikken i disse.

(134) I tillegg til de tekniske løsningene som brukes av leverandørene av AI-SYSTEMET, bør distributører som bruker et AI-SYSTEM til å generere eller manipulere bilde-, lyd- eller videoinnhold som i betydelig grad ligner på eksisterende personer, gjenstander, steder, enheter eller hendelser, og som feilaktig vil fremstå som autentisk eller sannferdig for en person (deep fakes), også klart og tydelig opplyse om at innholdet er kunstig skapt eller manipulert ved å merke i samsvar med dette og opplyse om deres kunstige opprinnelse. Overholdelse av denne plikten til åpenhet bør ikke tolkes som en indikasjon på at bruken AV aI-systemet eller dets resultater hindrer retten til ytringsfrihet og retten til frihet for kunst og vitenskap som er garantert i pakten, særlig der innholdet er en del av et åpenbart kreativt, satirisk, kunstnerisk, fiktivt analogt verk eller program, med forbehold om hensiktsmessige garantier for tredjeparters rettigheter og friheter. I slike tilfeller er plikten til åpenhet om etterligninger som er fastsatt i denne forordning, begrenset til å opplyse om eksistensen av slikt generert eller manipulert innhold på en hensiktsmessig måte som ikke hindrer visningen eller nytelsen av verket, herunder normal utnyttelse og bruk av det, samtidig som verkets nytteverdi og kvalitet opprettholdes. I tillegg er det også hensiktsmessig å se for seg en lignende opplysningsplikt I forbindelse med AI-genererte eller manipulerte tekster i DEN utstrekning de offentliggjøres med det formål å informere allmennheten om forhold av allmenn interesse, med mindre det AI-genererte innholdet har gjennomgått en prosess med menneskelig gjennomgang eller redaksjonell kontroll og en fysisk eller juridisk person har det redaksjonelle ansvaret for offentliggjøringen av innholdet.

(135) Uten at det berører åpenhetsforpliktelsenes obligatoriske karakter og fullstendige anvendelse, kan Kommisjonen også oppmuntre til og legge til rette for utarbeidelse av regler for god praksis på unionsplan for å legge til rette for en effektiv gjennomføring av forpliktelsene med hensyn til påvisning og merking av kunstig generert eller manipulert innhold, herunder for å støtte praktiske ordninger for, alt etter hva som er hensiktsmessig, å gjøre påvisningsmekanismene tilgjengelige og legge til rette for samarbeid med andre aktører i verdikjeden, spre innhold eller kontrollere dets autentisitet og opprinnelse for å gjøre det mulig for allmennheten å effektivt skille mellom innhold som er kunstig GENERERT.

(136) Forpliktelsene som i denne forordning pålegges tilbydere og distributører av visse AI-systemer for å gjøre det mulig å oppdage og avsløre at resultatene fra disse systemene er kunstig generert eller manipulert, er særlig relevante for å legge til rette for en effektiv gjennomføring av forordning (EU) 2022/2065. Dette gjelder særlig forpliktelsene til tilbydere av svært store nettbaserte plattformer eller svært store nettbaserte søkemotorer til å identifisere og avbøte systemiske risikoer som kan oppstå som følge av spredning av innhold som er kunstig generert eller manipulert, særlig risikoen for faktiske eller forutsigbare negative virkninger på demokratiske prosesser, samfunnsdebatt og valgprosesser, herunder gjennom desinformasjon. Kravet om å merke innhold som genereres AV KI-systemer i henhold til denne forordning, berører ikke plikten i artikkel 16 nr. 6 i forordning (EU) 2022/2065 for tilbydere av vertstjenester til å behandle meldinger om ulovlig innhold som mottas i henhold til artikkel 16 nr. 1 i nevnte forordning, og bør ikke påvirke vurderingen av og beslutningen om det spesifikke innholdets lovstridighet. Denne vurderingen bør utelukkende utføres med henvisning til reglene som regulerer innholdets lovlighet.

(137) Overholdelse av åpenhetsforpliktelsene for aI-systemene som omfattes av denne forordning, bør ikke tolkes som en indikasjon på at bruken av AI-SYSTEMET eller dets resultater er lovlig i henhold til denne forordning eller annen unionsrett eller medlemsstatenes nasjonale rett, og bør ikke berøre andre åpenhetsforpliktelser for brukere AV som er fastsatt i unionsretten eller nasjonal rett.

(138) aI er teknologifamilie I rask utvikling som krever regulatorisk tilsyn og et trygt og kontrollert rom for eksperimentering, samtidig som man sikrer ansvarlig innovasjon og integrering av passende sikkerhetstiltak og risikoreduserende tiltak. For å sikre et regelverk som fremmer innovasjon, er fremtidsrettet og motstandsdyktig mot forstyrrelser, bør medlemsstatene sørge for at deres nasjonale kompetente myndigheter oppretter minst én regulatorisk sandkasse for AI PÅ nasjonalt nivå for å legge rette for utvikling og testing av innovative aI-systemer under streng regulatorisk overvåking før disse systemene markedsføres eller på annen måte tas i bruk. Medlemsstatene kan også oppfylle denne forpliktelsen ved å delta i allerede eksisterende regulatoriske sandkasser eller etablere en sandkasse i fellesskap med én eller flere medlemsstaters vedkommende myndigheter, i den grad denne deltakelsen gir tilsvarende nasjonal dekning for de deltakende medlemsstatene. AI-REGULATORISKE sandkasser kan etableres i fysisk, digital eller hybrid form og kan omfatte både fysiske og digitale produkter. Etablerende myndigheter bør også sørge for at de regulatoriske sandkassene har tilstrekkelige ressurser til å fungere, herunder økonomiske og menneskelige ressurser.

(139) Målene med de regulatoriske sandkassene for KI bør være å fremme KI-innovasjon ved å etablere et kontrollert eksperiment- og testmiljø i utviklings- og førmarkedsføringsfasen med sikte på å sikre at de innovative KI-systemene er i samsvar med denne forordning og annen relevant unionsrett og nasjonal rett. Videre bør de regulatoriske sandkassene for aI-innovasjon ha som mål å styrke rettssikkerheten for innovatører og vedkommende myndigheters tilsyn med og forståelse av mulighetene, nye risikoer og virkningene av aI-bruk, å legge til rette for at myndigheter og foretak kan lære av regelverket, herunder med sikte på framtidige tilpasninger av den rettslige rammen, å støtte samarbeid og utveksling av beste praksis med de myndighetene som deltar i den regulatoriske sandkassen for aI-innovasjon, og å fremskynde markedsadgangen, blant annet ved å fjerne hindringer for små og mellomstore bedrifter, herunder nyetablerte foretak. Sandkasser for regulering bør være allment tilgjengelige i hele Unionen, og det bør legges særlig vekt på at de er tilgjengelige for små og mellomstore bedrifter, herunder oppstartsbedrifter. Deltakelsen i sandkassen for aI-regelverk bør fokusere på spørsmål som skaper rettslig usikkerhet for tilbydere og potensielle tilbydere, slik at de kan innovere, eksperimentere med AI i EU og bidra til evidensbasert læring om regelverk. Tilsynet med aI-systemene i den regulatoriske sandkassen for AI bør derfor omfatte utvikling, opplæring, testing og validering før systemene bringes i omsetning eller tas i bruk, samt begrepet og forekomsten av vesentlige endringer som kan kreve en ny framgangsmåte for samsvarsvurdering. alle vesentlige risikoer som identifiseres under utviklingen og testingen av slike AI-SYSTEMER, bør føre til tilstrekkelige risikoreduserende tiltak og, dersom dette ikke lykkes, til at utviklings- og testprosessen avbrytes. Der det er hensiktsmessig, bør nasjonale vedkommende myndigheter som oppretter regulatoriske sandkasser for aI, samarbeide med andre relevante myndigheter, herunder de som fører tilsyn med beskyttelsen AV grunnleggende rettigheter, og kan åpne for involvering av andre aktører i aI-økosystemet, f.eks. nasjonale eller europeiske , meldte organer, test- og forsøksfasiliteter, forsknings- og forsøkslaboratorier, europeiske digitale innovasjonssentre og relevante interessentorganisasjoner og organisasjoner i det sivile samfunn. For å sikre ensartet gjennomføring i hele Unionen og stordriftsfordeler bør det fastsettes felles regler for gjennomføringen av de regulatoriske sandkassene for AI og en ramme for samarbeid mellom relevante myndighetene som er involvert i tilsynet med sandkassene. AI-REGULATORISKE sandkasser som opprettes i henhold til denne forordning, bør ikke berøre annen lovgivning som åpner for opprettelse av andre sandkasser som har til formål å sikre overholdelse AV annen lovgivning enn denne forordning. Der det er hensiktsmessig, bør relevante vedkommende myndigheter med ansvar for disse andre regulatoriske sandkassene vurdere fordelene ved å bruke disse sandkassene også for å sikre at AI-systemer er I samsvar med denne forordning. Etter avtale mellom de nasjonale vedkommende myndigheter og deltakerne i den regulatoriske sandkassen for AI, kan testing under reelle forhold også drives og overvåkes innenfor rammen av den regulatoriske sandkassen FOR aI.

(140) Denne forordning bør gi rettslig grunnlag for at tilbydere og potensielle tilbydere i den regulatoriske sandkassen for KI kan bruke personopplysninger som er samlet inn til andre formål for å utvikle visse KI-systemer i allmennhetens interesse innenfor den regulatoriske sandkassen for KI, bare på nærmere angitte vilkår, i samsvar med artikkel 6 nr. 4 og artikkel 9 nr. 2 bokstav g) i forordning (EU) 2016/679 og artikkel 5, 6 og 10 i forordning (EU) 2018/1725, og uten at det berører artikkel 4 nr. 2 og artikkel 10 i direktiv (EU) 2016/680. alle andre forpliktelser for behandlingsansvarlige og rettigheter for registrerte i henhold til forordning (EU) 2016/679 og (EU) 2018/1725 og direktiv (EU) 2016/680 fortsatt får anvendelse. Denne forordningen skal særlig ikke gi et rettslig grunnlag i henhold artikkel 22 nr. 2 bokstav b) i forordning (EU) 2016/679 og artikkel 24 nr. 2 bokstav b) i forordning (EU) 2018/1725. Tilbydere og potensielle

tilbydere I den regulatoriske sandkassen FOR AI bør sørge for passende sikkerhetstiltak og samarbeide med vedkommende myndigheter, blant annet ved å følge deres veiledning og handle raskt og i god tro for å redusere eventuelle identifiserte betydelige risikoer for sikkerhet, helse og grunnleggende rettigheter som kan oppstå under utvikling, testing og eksperimentering i denne sandkassen, på en hensiktsmessig måte.

(141) For å fremskynde utviklingsprosessen og markedsføringen av høyrisikosystemer FOR kunstig INTELLIGENS SOM ER oppført et vedlegg til denne forordning, er det viktig at tilbydere eller potensielle tilbydere av slike systemer også kan dra nytte av en særlig ordning for utprøving av disse systemene under reelle forhold, uten å delta i en sandkasse for KUNSTIG INTELLIGENS. I slike tilfeller bør det imidlertid, idet det tas hensyn til de mulige konsekvensene av slik testing for enkeltpersoner, sikres at det ved denne forordning innføres hensiktsmessige og tilstrekkelige garantier og vilkår for tilbydere eller potensielle tilbydere. Slike garantier bør blant annet omfatte krav om informert samtykke fra fysiske personer til å delta testing under reelle forhold, med unntak av rettshåndhevelse der innhenting av informert samtykke vil hindre at AI-systemet blir testet. Samtykke fra forsøkspersoner til å delta i slik testing i henhold til denne forordningen skiller seg fra, og berører ikke, de registrertes samtykke til behandling av deres personopplysninger i henhold til relevant personvernlovgivning. Det er også viktig å minimere risikoene og muliggjøre tilsyn fra kompetente myndigheters side, og derfor kreves det at potensielle tilbydere har en plan for testing i virkelige verden som sendes inn til kompetent markedstilsynsmyndighet, at testingen registreres i egne seksjoner i EU-databasen, med visse begrensede unntak, at det fastsettes begrensninger for hvor lenge testingen kan utføres, og at det kreves ytterligere garantier for personer som tilhører visse sårbare grupper, samt at det inngås en skriftlig avtale som definerer rollene og ansvarsområdene til potensielle tilbydere og driftsansvarlige, og at kompetent personell som er involvert i testingen i den virkelige verden, fører effektivt tilsyn. Videre bør det fastsettes ytterligere sikkerhetstiltak for å sikre at KI-systemets spådommer, anbefalinger eller beslutninger effektivt kan reverseres og ignoreres, og at personopplysninger beskyttes og slettes når forsøkspersonene har trukket tilbake sitt samtykke til å delta i testingen, uten at det berører deres rettigheter som registrerte i henhold til Unionens personvernlovgivning. Når det gjelder overføring av data, er det også hensiktsmessig å se for seg at data som samles inn og behandles med henblikk på testing under reelle forhold, bare bør overføres til tredjestater der egnede og gjeldende garantier i henhold til unionsretten er gjennomført, særlig i samsvar med grunnlaget for overføring av personopplysninger i henhold til unionsretten om databeskyttelse, mens det for andre data enn personopplysninger treffes egnede garantier i samsvar med unionsretten, f.eks. europaparlaments- og rådsforordning (EU) 2022/868 [42] [(43)] og (EU) 2023/2854

(142) For å sikre at AI fører til sosialt og miljømessig fordelaktige resultater, oppfordres medlemsstatene til å støtte og fremme forskning og utvikling av aI-løsninger til støtte for sosialt og miljømessig fordelaktige resultater, for eksempel AI-BASERTE løsninger for å øke tilgjengeligheten for personer med nedsatt funksjonsevne, takle sosioøkonomiske ulikheter eller oppfylle miljømål, ved å bevilge tilstrekkelige ressurser, herunder offentlig finansiering og unionsfinansiering, og, der det er hensiktsmessig og forutsatt at støtteberettigelses- og utvelgelseskriteriene er oppfylt, særlig vurdere prosjekter som forfølger slike mål. Slike prosjekter bør være basert på prinsippet om tverrfaglig samarbeid mellom AI-utviklere, eksperter på ulikhet og ikke-diskriminering, tilgjengelighet, forbruker-, miljø- og digitale rettigheter, samt akademikere.

(143) For å fremme og beskytte innovasjon er det viktig at det tas særlig hensyn til interessene til små og mellomstore bedrifter, herunder nyetablerte bedrifter, som leverer eller TAR I BRUK AI-systemer. For dette formål bør medlemsstatene utvikle initiativer som er rettet mot disse operatørene, blant annet når det gjelder bevisstgjøring og informasjonsformidling. Medlemsstatene bør små og mellomstore bedrifter, herunder nyetablerte foretak, som har et registrert kontor eller en filial I Unionen, prioritert tilgang til de regulatoriske sandkassene for aI, forutsatt at de oppfyller vilkårene og utvelgelseskriteriene, og uten å utelukke andre tilbydere og potensielle tilbydere fra å få tilgang til sandkassene, forutsatt at de samme vilkårene og kriteriene er oppfylt. Medlemsstatene bør bruke eksisterende kanaler og, der det er hensiktsmessig, opprette nye dedikerte kanaler for kommunikasjon med små og mellomstore bedrifter, herunder oppstartsbedrifter, distributører, andre innovatører og, der det er hensiktsmessig, lokale offentlige myndigheter, for å støtte små og mellomstore bedrifter gjennom hele deres utviklingsløp ved å gi veiledning og svare på spørsmål om gjennomføringen av denne forordning. Der det er hensiktsmessig, bør disse kanalene samarbeide for å skape synergier og sikre ensartethet i veiledningen til små og mellomstore bedrifter, herunder nyetablerte bedrifter, og distributører. i tillegg bør medlemsstatene legge til rette for at små og mellomstore bedrifter og andre relevante interessenter kan delta i standardiseringsutviklingsprosessene. Dessuten bør det tas hensyn til de spesifikke interessene og behovene til leverandører som er små og mellomstore bedrifter,

(42) Europaparlaments- og rådsforordning (EU) 2022/868 av 30. mai 2022 om europeisk datastyring og om endring av forordning (EU) 2018/1724 (datastyringsloven) (EUT L 152 av 3.6.2022, s. 1).

(43) Europaparlaments- og rådsforordning (EU) 2023/2854 av 13. desember 2023 om harmoniserte regler om rettferdig tilgang til og bruk data og om endring av forordning (EU) 2017/2394 og direktiv (EU) 2020/1828 (datalov) (EUT L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

herunder nyetablerte bedrifter, bør tas i betraktning når meldte organer fastsetter gebyrer for samsvarsvurdering. Kommisjonen bør regelmessig vurdere sertifiserings- og samsvarskostnadene for små og mellomstore bedrifter, herunder nyetablerte bedrifter, gjennom åpne høringer, og bør samarbeide med medlemsstatene for å senke slike kostnader. For eksempel kan oversettelseskostnader knyttet til obligatorisk dokumentasjon og kommunikasjon med myndighetene utgjøre en betydelig kostnad for leverandører og andre operatører, særlig de i mindre skala. Medlemsstatene bør muligens sørge for at et av språkene de fastsetter og godtar for relevant dokumentasjon fra tilbydere og for kommunikasjon med operatører, er et språk som forstås av et størst mulig antall grenseoverskridende utbyggere. For å imøtekomme de spesifikke behovene til små og mellomstore bedrifter, herunder nyetablerte bedrifter, bør Kommisjonen på anmodning fra styret tilby standardiserte maler for de områdene som omfattes av denne forordningen. I tillegg bør Kommisjonen utfylle medlemsstatenes innsats ved å tilby en felles informasjonsplattform med brukervennlig informasjon om denne forordningen for alle tilbydere og utbyggere, ved å organisere egnede kommunikasjonskampanjer for å øke bevisstheten om forpliktelsene som følger av denne forordningen, og ved å evaluere og fremme konvergens av beste praksis i offentlige anskaffelsesprosedyrer I forbindelse med AI-systemer. Mellomstore foretak som inntil nylig kvalifiserte som små foretak i henhold til vedlegget til kommisjonsrekommandasjon 2003/361/EF ([44])bør ha tilgang til disse støttetiltakene, ettersom disse nye mellomstore foretakene noen ganger kan mangle de juridiske ressursene og den opplæringen som er nødvendig for å sikre riktig forståelse av og overholdelse av denne forordning.

(144) For å fremme og beskytte innovasjon, aI-on-demand-plattformen, bør alle relevante finansieringsprogrammer og -prosjekter i Unionen, f.eks. programmet for et digitalt Europa og Horisont Europa, som gjennomføres av Kommisjonen og medlemsstatene på unionsplan eller nasjonalt plan, etter behov bidra til å nå målene i denne forordning.

(145) For å minimere risikoen for gjennomføring som følge av kunnskap og ekspertise på markedet, samt for å gjøre det lettere for tilbydere, særlig små og mellomstore bedrifter, herunder nyetablerte foretak, og meldte organer å overholde sine forpliktelser i henhold til denne forordning, bør aI-on-demand-plattformen, de europeiske digitale innovasjonsknutepunktene og test- og forsøksfasilitetene som er opprettet av Kommisjonen og medlemsstatene på unionsplan eller nasjonalt plan, bidra til gjennomføringen av denne forordning. Innenfor sine respektive oppgaver og kompetanseområder KAN aI-on-demand-plattformen, de europeiske digitale innovasjonsknutepunktene og test- og forsøksfasilitetene gi særlig teknisk og vitenskapelig støtte til leverandører og meldte organer.

(146) I lys av at enkelte operatører er svært små, og for å sikre forholdsmessighet med hensyn til innovasjonskostnader, er det dessuten hensiktsmessig å tillate mikroforetak å oppfylle en av de mest kostbare forpliktelsene, nemlig å etablere et kvalitetsstyringssystem, på en forenklet måte, noe som vil redusere den administrative byrden og kostnadene for disse foretakene uten å påvirke beskyttelsesnivået og behovet for å oppfylle kravene til høyrisikosystemer. Kommisjonen bør utarbeide retningslinjer for å spesifisere elementene i kvalitetsstyringssystemet som mikroforetak skal oppfylle på denne forenklede måten.

(147) Det er hensiktsmessig at Kommisjonen i den grad det er mulig, legger til rette for at organer, grupper eller laboratorier som er opprettet eller akkreditert i henhold til relevant EU-harmoniseringsregelverk, og som utfører oppgaver i forbindelse med samsvarsvurdering av produkter eller utstyr som omfattes av nevnte EU-harmoniseringsregelverk, får tilgang til test- og forsøksfasiliteter. Dette gjelder særlig ekspertpaneler, ekspertlaboratorier og referanselaboratorier på området medisinsk utstyr i henhold til forordning (EU) 2017/745 og (EU) 2017/746.

(148) Denne forordningen bør etablere et styringsrammeverk som både gjør det mulig å samordne og støtte anvendelsen av denne forordningen på nasjonalt nivå, samt bygge opp kompetanse på unionsnivå og integrere interessenter PÅ KI-OMRÅDET. En effektiv gjennomføring og håndheving av denne forordningen krever et styringsrammeverk som gjør det mulig å koordinere og bygge opp sentral ekspertise på unionsnivå. AI-kontoret ble opprettet ved Kommisjonens beslutning ([45]) og har som oppgave å utvikle Unionens ekspertise og kapasitet på AI-OMRÅDET og å bidra gjennomføringen av unionsretten om AI. Medlemsstatene bør legge til rette for aI-kontorets oppgaver med sikte på å støtte utviklingen av Unionens ekspertise og kapasitet på unionsnivå og styrke det digitale indre markedets virkemåte. Videre bør det opprettes et styre bestående av representanter for medlemsstatene, et vitenskapelig panel for å integrere forskersamfunnet og et rådgivende forum for å bidra med innspill fra interessenter til av denne forordning, på unionsplan og nasjonalt plan. Utviklingen av Unionens ekspertise og

(44) Kommisjonens rekommandasjon av 6. mai 2003 om definisjonen av mikroforetak og små og mellomstore bedrifter (EUT L 124 av 20.5.2003, s. 36).

(45) Kommisjonens beslutning av 24.1.2024 om opprettelse av European artificial Intelligence Office C(2024) 390.

kapasiteten bør også omfatte utnyttelse af eksisterende ressurser og ekspertise, særlig gjennom synergier med strukturer som er bygget opp I forbindelse med håndheving av annen lovgivning på unionsnivå, og synergier med beslektede initiativer på unionsnivå, som fellesforetaket EuroHPC og test- og eksperimenteringsfasilitetene FOR KUNSTIG INTELLIGENS under programmet for ET digitalt Europa.

(149) For å legge til rette for en smidig, effektiv og harmonisert gjennomføring av denne forordning bør det opprettes et styre. Styret bør gjenspeile de ulike interessene I AI-økosystemet og være sammensatt av representanter for . Styret bør ha ansvar for en rekke rådgivende oppgaver, herunder å avgi uttalelser, anbefalinger, råd eller bidra til veiledning i saker som gjelder gjennomføringen av denne forordning, herunder håndhevingsspørsmål, tekniske spesifikasjoner eller eksisterende standarder vedrørende kravene fastsatt i denne forordning, og å gi råd til Kommisjonen og medlemsstatene og deres nasjonale vedkommende myndigheter om særlige spørsmål knyttet til AI. For å gi medlemsstatene en viss fleksibilitet i utpekingen av sine representanter i styret, kan disse representantene være personer som tilhører offentlige organer, og som bør ha relevant kompetanse og fullmakter til å lette samordningen på nasjonalt plan og bidra til at styret kan utføre sine oppgaver. Styret bør opprette to faste undergrupper for å skape en plattform for samarbeid og utveksling mellom markedstilsynsmyndigheter og notifiserende myndigheter om spørsmål knyttet til henholdsvis markedstilsyn og notifiserte organer. Den stående undergruppen for markedstilsyn bør fungere som den administrative samarbeidsgruppen (adCO) denne forordning i henhold til artikkel 30 i forordning (EU) 2019/1020. I samsvar med artikkel 33 i nevnte forordning bør Kommisjonen støtte virksomheten til den stående undergruppen for markedstilsyn ved å foreta markedsevalueringer eller -undersøkelser, særlig med sikte på å identifisere aspekter ved denne forordning som krever særlig og presserende samordning mellom markedstilsynsmyndighetene. Styret kan opprette andre faste eller midlertidige undergrupper etter behov for å undersøke særlige spørsmål. Personvernrådet bør også, der det er hensiktsmessig, samarbeide med relevante unionsorganer, ekspertgrupper og nettverk som er aktive i forbindelse med relevant unionsrett, herunder særlig de som er aktive i henhold til relevant unionsrett om data, digitale produkter og tjenester.

(150) For å sikre at interessentene involveres i gjennomføringen og anvendelsen denne forordning, bør det opprettes et rådgivende forum som skal gi råd og teknisk sakkunnskap til styret og Kommisjonen. For å sikre en variert og balansert interesserepresentasjon mellom kommersielle og ikke-kommersielle interesser og, innenfor kategorien kommersielle interesser, med hensyn til små og mellomstore bedrifter og andre foretak, bør det rådgivende forumet blant annet omfatte industrien, nyetablerte foretak, små og mellomstore bedrifter, den akademiske verden, det sivile samfunn, herunder partene i arbeidslivet, samt Byrået for grunnleggende rettigheter, ENISA, Den europeiske standardiseringskomité (CEN), Den europeiske komité for elektroteknisk standardisering (CENELEC) og Det europeiske standardiseringsinstituttet for telekommunikasjon (ETSI).

(151) For å støtte gjennomføringen og AV denne forordning, særlig overvåkingsvirksomheten til aI-kontoret med hensyn til generelle aI-modeller, bør det opprettes et vitenskapelig panel bestående av uavhengige eksperter. De uavhengige ekspertene som utgjør det vitenskapelige panelet, bør velges på grunnlag av oppdatert vitenskapelig eller teknisk sakkunnskap PÅ KI-området og bør utføre sine oppgaver upartisk og objektivt og sikre konfidensialiteten til informasjon og data som innhentes i forbindelse med utførelsen av deres oppgaver og virksomhet. For å gjøre det mulig å styrke den nasjonale kapasiteten som er nødvendig for en effektiv av denne forordning, bør medlemsstatene kunne anmode om støtte fra ekspertgruppen som utgjør det vitenskapelige panelet, til sine håndhevingsaktiviteter.

(152) For å støtte adekvat håndheving med hensyn til AI-SYSTEMER og styrke kapasiteten I , bør det opprettes støttestrukturer for aI-testing I Unionen, og disse bør gjøres tilgjengelige for medlemsstatene.

(153) Medlemsstatene har en nøkkelrolle i anvendelsen og håndhevingen av denne forordning. I denne forbindelse bør hver medlemsstat utpeke minst én meldermyndighet og minst én markedstilsynsmyndighet som nasjonale vedkommende myndigheter for å føre tilsyn med anvendelsen og gjennomføringen av denne forordning. Medlemsstatene kan beslutte å utpeke en hvilken som helst form for offentlig enhet til å utføre de nasjonale vedkommende myndigheters oppgaver i henhold til denne forordning, i samsvar med sine spesifikke nasjonale organisatoriske særtrekk og behov. For å øke effektiviteten i organiseringen fra medlemsstatenes side og for å etablere et felles overfor offentligheten og andre motparter på medlemsstats- og unionsnivå, bør hver utpeke en markedstilsynsmyndighet som skal fungere som et felles kontaktpunkt.

(154) De nasjonale vedkommende myndigheter bør utøve sine fullmakter uavhengig, upartisk og upartisk, slik at prinsippene om objektivitet i deres virksomhet og oppgaver ivaretas, og slik at anvendelsen og gjennomføringen av denne forordning sikres. Medlemmene av disse myndighetene bør avstå fra enhver handling som er uforenlig med deres oppgaver, og bør være underlagt taushetsplikt i henhold til denne forordning.

(155) For å sikre at leverandører AV høyrisiko-AI-systemer kan ta hensyn til erfaringene med bruk AV høyrisiko-AI-systemer for å forbedre sine systemer og design- og utviklingsprosessen, eller kan iverksette eventuelle korrigerende tiltak i tide, bør alle leverandører ha et system for overvåking etter at utstyret er brakt i omsetning. Der det er relevant, bør overvåking etter markedsføring omfatte en analyse av samspillet med andre aI-systemer, inkludert annet utstyr og annen programvare. Overvåking etter markedsføring bør ikke omfatte sensitive driftsdata fra brukere som er rettshåndhevende myndigheter. Dette systemet er også viktig for å sikre at mulige risikoer som oppstår fra aI-systemer som fortsetter å "lære" etter at de er brakt i omsetning eller tatt i bruk, kan håndteres mer effektivt og i tide. I denne sammenheng bør det også kreves at leverandørene har et system for å rapportere relevante myndigheter om alvorlige hendelser som skyldes bruken av deres , det vil si hendelser eller funksjonsfeil som fører til dødsfall eller alvorlig helseskade, alvorlige og irreversible forstyrrelser i forvaltningen og driften av kritisk infrastruktur, brudd på forpliktelser i henhold til unionsretten som har til hensikt å beskytte grunnleggende rettigheter, eller alvorlig skade på eiendom eller miljø.

(156) For å sikre en hensiktsmessig og effektiv håndheving av kravene og forpliktelsene fastsatt i denne forordning, som Unionens harmoniseringsregelverk, bør systemet markedstilsyn og etterlevelse av produkter som er etablert ved forordning (EU) 2019/1020, få anvendelse i sin helhet. Markedstilsynsmyndigheter som er utpekt i henhold til denne forordning, bør ha alle håndhevingsbeføyelser som er fastsatt i denne forordning og i forordning (EU) 2019/1020, og bør utøve sine fullmakter og utføre sine oppgaver på en uavhengig, upartisk og upartisk måte. Selv om de fleste KI-systemer ikke er underlagt særlige krav og forpliktelser i henhold til denne forordning, kan markedstilsynsmyndighetene treffe tiltak i forbindelse med alle KI-systemer når de utgjør en risiko i samsvar med denne forordning. på grunn av den særlige karakteren unionsinstitusjoner, -byråer og -organer som omfattes av denne forordnings virkeområde, er det hensiktsmessig å utpeke Den europeiske datatilsynsmann som vedkommende markedstilsynsmyndighet for dem. Dette bør ikke berøre medlemsstatenes utpeking av nasjonale vedkommende myndigheter. Markedstilsynsvirksomheten bør ikke påvirke de overvåkede enhetenes evne til å utføre sine oppgaver uavhengig, når slik uavhengighet er påkrevd i henhold til unionsretten.

(157) Denne forordning berører ikke kompetansen, oppgavene, beføyelsene og uavhengigheten til relevante nasjonale offentlige myndigheter eller organer som fører tilsyn med anvendelsen av unionsretten om beskyttelse av grunnleggende rettigheter, herunder likestillingsorganer og personvernmyndigheter. Dersom det er nødvendig for deres mandat, bør disse nasjonale offentlige myndighetene eller organene også ha tilgang til all dokumentasjon som er utarbeidet i henhold til denne forordning. Det bør fastsettes EN særlig for å sikre tilstrekkelig og rettidig håndheving mot KI-systemer som utgjør en risiko for helse, sikkerhet og grunnleggende rettigheter. Prosedyren for slike KI-systemer som utgjør en risiko, bør anvendes på KI-SYSTEMER med høy risiko som utgjør en risiko, forbudte systemer som er brakt i , tatt i bruk eller brukt I strid med den forbudte praksisen fastsatt I denne forordning, og KI-systemer som er gjort tilgjengelige I strid med åpenhetskravene fastsatt i denne forordning, og som utgjør en risiko.

(158) Unionens lovgivning om finansielle tjenester omfatter interne regler og krav for styring og risikohåndtering som får anvendelse på regulerte finansinstitusjoner I forbindelse med ytelsen av disse tjenestene, herunder når de BRUKER KI-systemer. For å sikre ensartet anvendelse og håndheving av forpliktelsene i henhold til denne forordning og relevante regler og krav i Unionens rettsakter om finansielle tjenester skal vedkommende myndigheter for tilsyn og håndheving av disse rettsaktene, særlig vedkommende myndigheter som definert i europaparlaments- og rådsforordning (EU) nr. 575/2013 [46]) og direktiv 2008/48/EF [47], 2009/138/EF [48].)

(46) Europaparlaments- og rådsforordning (EU) nr. 575/2013 av 26. juni 2013 om tilsynskrav for kredittinstitusjoner og verdipapirforetak og om endring av forordning (EU) nr. 648/2012 (EUT L 176 av 27.6.2013, s. 1).

(47) europaparlaments- og rådsdirektiv 2008/48/EF av 23. april 2008 om kredittavtaler for forbrukere og om opphevelse av rådsdirektiv 87/102/EØF (EUT L 133 av 22.5.2008, s. 66).

(48) Europaparlaments- og rådsdirektiv 2009/138/EF av 25. november 2009 om adgang til og av forsikrings- og gjenforsikringsvirksomhet (Solvens II) (EUT L 335 av 17.12.2009, s. 1).

2013/36/EU ([49]), 2014/17/EU ([50]) og (EU) 2016/97 ([51]) fra Europaparlamentet og Rådet bør, innenfor sine respektive kompetanseområder, utpekes som vedkommende myndigheter med henblikk på å føre tilsyn med gjennomføringen av denne forordning, herunder for markedstilsynsvirksomhet, med hensyn til AI-systemer som leveres eller brukes av finansinstitusjoner som ER underlagt regulering og tilsyn, med mindre beslutter utpeke en annen myndighet til å utføre disse markedstilsynsoppgavene. Disse vedkommende myndigheter bør ha all myndighet i henhold til denne forordning og forordning (EU) 2019/1020 til å håndheve kravene og forpliktelsene i denne forordning, herunder myndighet til å utføre *etterfølgende* markedstilsynsaktiviteter som, alt etter hva som er hensiktsmessig, kan integreres i deres eksisterende tilsynsmekanismer og -prosedyrer i henhold til den relevante unionsretten om finansielle tjenester. Det er hensiktsmessig å se for seg at nasjonale myndigheter med ansvar for tilsyn med kredittinstitusjoner som er regulert i henhold til direktiv 2013/36/EU, og som deltar i den felles tilsynsmekanismen opprettet ved rådsforordning ((52, EU) nr. 1024/2013)når de opptrer som markedstilsynsmyndigheter i henhold til denne forordninguten opphold bør rapportere til Den europeiske sentralbank all informasjon som er identifisert i løpet av deres markedstilsynsvirksomhet, og som kan være av potensiell interesse for Den europeiske sentralbanks tilsynsoppgaver som angitt i nevnte forordning. For ytterligere å styrke sammenhengen mellom denne forordning og reglene som gjelder for kredittinstitusjoner som er regulert i henhold til direktiv 2013/36/EU, er det også hensiktsmessig å integrere noen av tilbydernes prosedyreforpliktelser i forbindelse med risikohåndtering, overvåking etter markedsføring og dokumentasjon i de eksisterende forpliktelsene og prosedyrene i henhold til direktiv 2013/36/EU. For å unngå overlapping bør det også fastsettes begrensede unntak for tilbydernes kvalitetsstyringssystem og overvåkingsplikten som påhviler dem som tar i bruk høyrisikosystemer, I DEN grad disse gjelder for kredittinstitusjoner som er regulert AV direktiv 2013/36/EU. Den samme ordningen bør gjelde for forsikrings- og gjenforsikringsforetak og forsikringsholdingselskaper i henhold til direktiv 2009/138/EF og forsikringsformidlere i henhold til direktiv (EU) 2016/97 og andre typer finansinstitusjoner som er underlagt krav til intern styring, ordninger eller prosesser fastsatt i henhold til den relevante unionsretten om finansielle tjenester for å sikre konsekvens og likebehandling i finanssektoren.

(159) Hver markedstilsynsmyndighet for høyrisiko-AI-systemer på området biometri, som er oppført i et vedlegg til denne forordning, i den grad disse systemene brukes i forbindelse med rettshåndhevelse, migrasjon, asyl- og grensekontrollforvaltning eller rettspleie og demokratiske prosesser, bør ha effektive undersøkelses- og , herunder minst myndighet til å få tilgang til alle personopplysninger som behandles, og til all informasjon som er nødvendig for at den skal kunne sine oppgaver. Markedstilsynsmyndighetene bør kunne utøve sine fullmakter ved å opptre fullstendig uavhengig. Eventuelle begrensninger av deres tilgang til sensitive driftsdata i henhold til denne forordning bør ikke berøre de fullmakter de er tillagt ved direktiv (EU) 2016/680. Ingen utelukkelse av utlevering av opplysninger til nasjonale datatilsynsmyndigheter i henhold til denne forordning bør påvirke disse myndighetenes nåværende eller framtidige myndighet utover denne forordnings virkeområde.

(160) Markedstilsynsmyndighetene og Kommisjonen bør kunne foreslå felles aktiviteter, herunder felles undersøkelser, som skal gjennomføres av markedstilsynsmyndighetene eller markedstilsynsmyndighetene sammen med Kommisjonen, og som har som mål å fremme etterlevelse, identifisere manglende etterlevelse, øke bevisstheten og gi veiledning i forbindelse med denne forordning med hensyn til bestemte kategorier AV høyrisiko-AI-systemer som HAR vist seg å utgjøre en alvorlig risiko i to eller flere medlemsstater. Felles aktiviteter for å fremme etterlevelse bør gjennomføres i samsvar med artikkel 9 i forordning (EU) 2019/1020. aI-kontoret bør gi koordineringsstøtte til felles etterforskninger.

(161) Det er nødvendig å klargjøre ansvars- og kompetanseforholdene på unionsnivå og nasjonalt nivå når det gjelder aI-systemer som er bygget på generelle . For å unngå overlappende kompetanse, der et aI-system er basert en generell aI-modell og modellen og systemet leveres av samme leverandør, bør tilsynet

(49) Europaparlaments- og rådsdirektiv 2013/36/EU av 26. juni 2013 om adgang til å utøve virksomhet i og om tilsyn med kredittinstitusjoner og verdipapirforetak, om endring av direktiv 2002/87/EF og om oppheving av direktiv 2006/48/EF og 2006/49/EF (EUT L 176 av 27.6.2013, s. 338).

(50) Europaparlaments- og rådsdirektiv 2014/17/EU av 4. februar 2014 om kredittavtaler for forbrukere knyttet til boligeiendom og om endring av direktiv 2008/48/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 (EUT L 60 av 28.2.2014, s. 34).

(51) Europaparlaments- og rådsdirektiv (EU) 2016/97 av 20. januar 2016 om forsikringsdistribusjon (EUT L 26 av 2.2.2016, s. 19).

(52) Rådsforordning (EU) nr. 1024/2013 av 15. oktober 2013 om overføring av særlige oppgaver til Den europeiske sentralbank i forbindelse med politikken for tilsyn med kredittinstitusjoner (EUT L 287 av 29.10.2013, s. 63).

finne sted på unionsnivå gjennom aI-kontoret, som for dette formålet bør ha myndighet som en markedstilsynsmyndighet I henhold til forordning (EU) 2019/1020. I alle andre tilfeller forblir nasjonale markedstilsynsmyndigheter ansvarlige for tilsynet med . For allmenne aI-systemer som kan brukes direkte av distributører til minst ett formål som er klassifisert som høyrisiko, bør imidlertid markedstilsynsmyndighetene samarbeide med aI-kontoret for å gjennomføre evalueringer av samsvar og informere styret og andre markedstilsynsmyndigheter om dette. Videre bør markedstilsynsmyndighetene kunne be om bistand fra aI-kontoret i tilfeller der markedstilsynsmyndigheten ikke er I stand til å avslutte en undersøkelse et høyrisiko aI-system på grunn av manglende tilgang til visse opplysninger knyttet til den generelle AI-MODELLEN som høyrisiko aI-systemet er bygget på. I slike tilfeller bør framgangsmåten for gjensidig bistand i grenseoverskridende saker i kapittel VI i forordning (EU) 2019/1020 få *tilsvarende* anvendelse.

(162) For å utnytte den sentraliserte unionsekspertisen og synergiene på unionsplan best mulig, bør Kommisjonen ha myndighet til å føre tilsyn med og håndheve forpliktelsene for tilbydere AV generelle AI-MODELLER. AI-kontoret bør kunne gjennomføre alle tiltak som er nødvendige for å overvåke den faktiske gjennomføringen av denne forordning med hensyn til generelle aI-modeller. Det bør kunne undersøke mulige av reglene for tilbydere av generelle AI-MODELLER både på eget initiativ, på grunnlag av resultatene av sine overvåkingsaktiviteter eller på anmodning fra markedstilsynsmyndigheter i samsvar med vilkårene fastsatt i denne forordning. For å støtte effektiv overvåking AV aI-kontoret bør den gi nedstrømsleverandører mulighet til å inngi klager på mulige overtredelser av reglene for tilbydere AV generelle aI-modeller og -systemer.

(163) For å utfylle styringssystemene for generelle aI-modeller bør det vitenskapelige panelet støtte overvåkingsaktivitetene til aI-kontoret og kan i visse tilfeller gi kvalifiserte varsler til som utløser oppfølging, for eksempel undersøkelser. Dette bør være tilfelle når det vitenskapelige panelet har grunn til å mistenke at en generell aI-modell utgjør en konkret og identifiserbar risiko på unionsnivå. Videre bør dette være tilfelle når det vitenskapelige panelet har grunn til å mistenke at en generell aI-modell oppfyller kriteriene som vil føre til en klassifisering som en generell aI-modell med systemrisiko. For å utstyre det vitenskapelige panelet med den informasjonen som er nødvendig for å utføre disse oppgavene, bør det finnes en mekanisme som gjør det mulig for det vitenskapelige panelet å anmode Kommisjonen om å kreve dokumentasjon eller informasjon fra en leverandør.

(164) AI-kontoret bør kunne treffe de tiltak som er nødvendige for å overvåke den faktiske gjennomføringen og overholdelsen av forpliktelsene for tilbydere AV generelle AI-modeller fastsatt i denne forordning. AI-kontoret bør kunne undersøke mulige overtredelser i samsvar med de fullmakter som er fastsatt i denne forordning, herunder ved å anmode om dokumentasjon og informasjon, ved å gjennomføre evalueringer og ved å anmode om tiltak fra tilbydere AV allsidige AI-modeller. For å kunne gjøre bruk av uavhengig ekspertise bør aI-kontoret kunne involvere uavhengige eksperter til å utføre evalueringene på sine vegne når det foretar evalueringer. Overholdelse av forpliktelsene bør kunne håndheves, blant annet gjennom anmodninger om å treffe egnede tiltak, herunder risikoreduserende tiltak i tilfelle identifiserte systemrisikoer samt begrensning av tilgjengeliggjøringen på markedet, tilbaketrekking eller tilbakekalling av modellen. som en garanti, om nødvendig utover de prosessuelle rettighetene fastsatt i denne forordning, bør tilbydere AV allmenne AI-MODELLER ha de prosessuelle rettighetene fastsatt I artikkel 18 i forordning (EU) 2019/1020, som bør få *tilsvarende* anvendelse, uten at det berører mer spesifikke prosessuelle rettigheter fastsatt i denne forordning.

(165) Utviklingen av andre aI-systemer enn HØYRISIKO-AI-SYSTEMER i samsvar med kravene i denne forordning kan føre til en større utbredelse av etiske og pålitelige aI-systemer i Unionen. Tilbydere av aI-systemer som ikke er høyrisikosystemer, bør oppfordres til å utarbeide atferdsregler, herunder tilhørende styringsmekanismer, som har til hensikt å fremme frivillig anvendelse av noen av eller alle de obligatoriske kravene som gjelder for for aI, tilpasset i lys av det tiltenkte formålet med systemene og den lavere risikoen som er involvert, og idet det tas hensyn til de tilgjengelige tekniske løsningene og beste praksis i bransjen, f.eks. modell- og datakort. Tilbydere og, der det er hensiktsmessig, brukere av alle aI-systemer, høyrisikosystemer eller ikke, og aI-modeller bør også oppfordres til å anvende tilleggskrav på frivillig basis, for eksempel knyttet til elementene i Unionens etiske retningslinjer for pålitelig AI,

miljømessig bærekraft, tiltak for å øke kunnskapen om aI, inkluderende og mangfoldig utforming og utvikling av aI-systemer, herunder hensynet til sårbare personer og tilgjengelighet for personer med nedsatt funksjonsevne, interessentdeltakelse med involvering, der det er hensiktsmessig, av relevante interessenter som næringslivs- og sivilsamfunnsorganisasjoner, akademia, forskningsorganisasjoner, fagforeninger og forbrukervernorganisasjoner i utformingen og utviklingen av aI-systemer, og mangfold i utviklingsteamene, herunder kjønnsbalanse. For å sikre at de frivillige atferdsreglene er effektive, bør de være basert på klare mål og viktige resultatindikatorer for å måle oppnåelsen av disse målene. De bør også utvikles på en inkluderende måte, der det er hensiktsmessig, med involvering av relevante interessenter som næringsliv og organisasjoner i det sivile samfunn, akademia, forskningsorganisasjoner, fagforeninger og forbrukervernorganisasjoner. Kommisjonen kan utvikle initiativer, også av sektorspesifikk art, for å legge til rette for Å senke de tekniske hindringene som hindrer utveksling AV data OVER landegrensene for utvikling AV AI, herunder om infrastruktur for datatilgang, semantisk og teknisk interoperabilitet mellom ulike typer data.

(166) Det er viktig at KI-systemer knyttet til produkter som ikke er høyrisikoprodukter I henhold til denne forordningen, og som dermed ikke er pålagt å oppfylle kravene som ER fastsatt for høyrisikosystemer, likevel er trygge når de bringes i omsetning eller tas i bruk. For å bidra til dette målet vil europaparlaments- og rådsforordning (EU) 2023/988 ([53]) .gjelde som et sikkerhetsnett

(167) For å sikre et tillitsfullt og konstruktivt samarbeid mellom vedkommende myndigheter på unionsplan og nasjonalt plan bør alle parter som er involvert i anvendelsen av denne forordning, respektere konfidensialiteten til informasjon og opplysninger som er innhentet i forbindelse med utførelsen av deres oppgaver, i samsvar med unionsretten eller nasjonal rett. De bør utføre sine oppgaver og sin virksomhet på en slik måte at de særlig beskytter immaterielle rettigheter, fortrolige forretningsopplysninger og forretningshemmeligheter, den effektive gjennomføringen av denne forordning, offentlige og nasjonale sikkerhetsinteresser, integriteten til straffeprosesser og administrative prosesser og integriteten til sikkerhetsgradert informasjon.

(168) Etterlevelse av denne forordning bør kunne håndheves ved ileggelse av sanksjoner og andre håndhevingstiltak. Medlemsstatene bør treffe alle nødvendige tiltak for å sikre at bestemmelsene i denne forordning gjennomføres, herunder ved å fastsette effektive, forholdsmessige og avskrekkende sanksjoner for overtredelse av dem, og for å respektere *ne bis in* idem-prinsippet. For å styrke og harmonisere de administrative sanksjonene for overtredelse av denne forordning bør det fastsettes øvre grenser for fastsettelse av administrative bøter for visse spesifikke overtredelser. Ved fastsettelse av bøtenes størrelse bør medlemsstatene i hvert enkelt tilfelle ta hensyn til alle relevante omstendigheter i den konkrete situasjonen, særlig med behørig hensyn til overtredelsens art, alvorlighetsgrad og varighet og konsekvensene av den samt leverandørens størrelse, særlig dersom leverandøren er en SMB, herunder en nystartet virksomhet. Den europeiske datatilsynsmann bør ha myndighet til å ilegge unionsinstitusjoner, -byråer og -organer som omfattes av denne forordning, bøter.

(169) Overholdelse AV forpliktelsene som pålegges tilbydere av allsidige AI-modeller i henhold til denne forordning, bør kunne håndheves blant annet ved hjelp av bøter. For dette formål bør det også fastsettes passende bøtenivåer for overtredelse av disse forpliktelsene, herunder manglende overholdelse av tiltak som Kommisjonen har anmodet om i samsvar med denne forordning, med forbehold for passende foreldelsesfrister i samsvar med forholdsmessighetsprinsippet. Alle beslutninger som Kommisjonen treffer i henhold til denne forordning, kan prøves av Den europeiske unions domstol i samsvar med TEUV, herunder Domstolens ubegrensede myndighet med hensyn til sanksjoner i henhold til artikkel 261 i TEUV.

(170) Unionsretten og nasjonal rett gir allerede effektive rettsmidler til fysiske og juridiske personer hvis rettigheter og friheter påvirkes negativt av bruken AV AI-systemer. Uten at det berører disse rettsmidlene, bør enhver fysisk eller juridisk person som har grunn til å anta at det har funnet sted en overtredelse av denne forordning, ha rett til å inngi en klage til den relevante markedstilsynsmyndigheten.

(171) Berørte personer bør ha rett til å få en forklaring når en beslutning fra en driftsansvarlig hovedsakelig er basert på resultatene fra visse høyrisikosystemer som faller inn under denne forordningens virkeområde, og når denne beslutningen har rettsvirkninger eller på tilsvarende måte i betydelig grad påvirker disse personene PÅ en måte som de anser å ha en negativ

(53) Europaparlaments- og rådsforordning (EU) 2023/988 av 10. mai 2023 om generell produktsikkerhet, om endring av europaparlaments- og rådsforordning (EU) nr. 1025/2012 og europaparlaments- og rådsdirektiv (EU) 2020/1828 og om oppheving av europaparlaments- og rådsdirektiv 2001/95/EF og rådsdirektiv 87/357/EØF (EUT L 135 av 23.5.2023, s. 1).

innvirkning på deres helse, sikkerhet eller grunnleggende rettigheter. Forklaringen bør være klar og meningsfull og bør gi et grunnlag som gjør det mulig for de berørte personene å utøve sine rettigheter. Retten til å få en forklaring bør ikke gjelde for bruk AV AI-systemer som det følger unntak eller begrensninger for I unionsretten eller nasjonal rett, og bør bare gjelde i den utstrekning denne retten ikke allerede er fastsatt i unionsretten.

(172) Personer som varsler om overtredelser av denne forordning, bør være beskyttet i henhold til unionsretten. Europaparlaments- og rådsdirektiv (EU) 2019/1937 [54]) bør derfor få anvendelse på rapportering av overtredelser av denne forordning og beskyttelsen av personer som rapporterer slike overtredelser.

(173) For å sikre at regelverket kan tilpasses der det er nødvendig, bør myndigheten til å vedta rettsakter i samsvar med artikkel 290 i TEUV delegeres til Kommisjonen for å endre vilkårene for at et KI-system ikke skal anses for å være et , listen over høyrisikosystemer FOR KI, bestemmelsene om teknisk dokumentasjon, innholdet i EU-samsvarserklæringen, bestemmelsene om framgangsmåtene for samsvarsvurdering, bestemmelsene som fastsetter hvilke HØYRISIKO-AI-SYSTEMER som prosedyren for samsvarsvurdering basert på vurdering av kvalitetsstyringssystemet og vurdering av den tekniske dokumentasjonen skal gjelde for, terskelen, referanseverdiene og indikatorene, herunder ved å supplere disse referanseverdiene og indikatorene, i reglene for klassifisering av generelle FORMÅLS-AI-MODELLER med systemrisiko, kriteriene for utpeking av generelle formåls-AI-modeller med systemrisiko, den tekniske dokumentasjonen for tilbydere av generelle formåls-AI-modeller og informasjonen om åpenhet for tilbydere av generelle formåls-AI-modeller. Det er særlig viktig at Kommisjonen gjennomfører hensiktsmessige konsultasjoner under sitt forberedende arbeid, herunder på ekspertnivå, og at disse konsultasjonene gjennomføres i samsvar med prinsippene fastsatt i den interinstitutionelle avtalen av 13. april 2016 om bedre lovgivning ([55].) For å sikre likeverdig deltakelse i utarbeidelsen av delegerte rettsakter mottar Europaparlamentet og Rådet alle dokumenter samtidig med medlemsstatenes eksperter, og deres eksperter har systematisk tilgang til møter i Kommisjonens ekspertgrupper som arbeider med utarbeidelsen av delegerte rettsakter.

(174) Med tanke på den raske teknologiske utviklingen og den tekniske ekspertisen som kreves for å anvende denne forordning effektivt, bør Kommisjonen evaluere og gjennomgå denne forordning innen 2. august 2029 og deretter hvert fjerde år og rapportere til Europaparlamentet og Rådet. I tillegg bør Kommisjonen, idet det tas hensyn til konsekvensene denne forordnings virkeområde, foreta en vurdering av behovet for å endre listen over høyrisikosystemer og listen over forbudt praksis én gang i året. Videre bør Kommisjonen innen 2. august 2028 og deretter hvert fjerde år vurdere og rapportere til Europaparlamentet og Rådet om behovet for å endre listen over høyrisikoområder i vedlegget til denne forordning, AI-SYSTEMENE som omfattes av gjennomsiktighetsforpliktelsene, effektiviteten av tilsyns- og styringssystemet og framdriften i utviklingen av standardiseringsleveranser om energieffektiv utvikling av generelle aI-modeller, herunder behovet for ytterligere tiltak eller handlinger. Endelig bør Kommisjonen innen 2. august 2028 og deretter hvert tredje år evaluere virkningen og effektiviteten av frivillige atferdsregler for å fremme av kravene til HØYRISIKO-AI-SYSTEMER på andre AI-systemer enn HØYRISIKO-AI-SYSTEMER, og eventuelt andre tilleggskrav for slike AI-systemer.

(175) For å sikre ensartede vilkår for gjennomføringen av denne forordning bør Kommisjonen tildeles gjennomføringsmyndighet. Denne myndighet bør utøves i samsvar med europaparlaments- og rådsforordning (EU) nr. 182/2011 ([56].)

(176) Ettersom målet med denne forordning, nemlig å forbedre det indre markedets virkemåte og fremme innføringen av menneskefokusert og pålitelig AI, samtidig som det sikres et høyt nivå for beskyttelse av helse, sikkerhet, grunnleggende rettigheter som ER nedfelt i pakten, herunder demokrati, rettsstatsprinsipper og miljøvern mot skadelige virkninger AV AI-systemer i Unionen, og støtte innovasjon, ikke i tilstrekkelig grad kan oppnås av medlemsstatene og snarere, på grunn av tiltakets omfang eller virkninger, kan oppnås bedre på unionsplan, kan Unionen vedta

(54) Europaparlaments- og rådsdirektiv (EU) 2019/1937 av 23. oktober 2019 om beskyttelse av personer som melder fra om brudd på unionsretten (EUT L 305 av 26.11.2019, s. 17).

(55) EUT L 123 av 12.5.2016, s. 1.

(56) Europaparlaments- og rådsforordning (EU) nr. 182/2011 av 16. februar 2011 om fastsettelse av generelle regler og prinsipper for ordningen for medlemsstatenes kontroll med Kommisjonens av gjennomføringsmyndighet (EUT L 55 av 28.2.2011, s. 13).

tiltak i samsvar med nærhetsprinsippet som fastsatt i artikkel 5 i TEU. I samsvar med forholdsmessighetsprinsippet som fastsatt i samme artikkel, går denne forordning ikke lenger enn det som er nødvendig for å nå dette målet.

(177) For å sikre rettssikkerhet, sikre en passende tilpasningsperiode for driftsansvarlige og unngå forstyrrelser på markedet, herunder ved å sikre kontinuitet I bruken AV KI-systemer, bør denne forordning få anvendelse på høyrisiko KI-SYSTEMER som er brakt i omsetning eller tatt i før den generelle anvendelsesdatoen for forordningen, bare dersom disse systemene fra og med denne datoen er gjenstand for vesentlige endringer i sin utforming eller sitt tiltenkte formål. Det bør klargjøres at begrepet vesentlig endring i denne forbindelse bør forstås som innholdsmessig ekvivalent med begrepet vesentlig endring, som bare brukes med hensyn til høyrisikosystemer FOR KUNSTIG INTELLIGENS I henhold til denne forordning. Unntaksvis og i lys av offentlig ansvarlighet bør operatører AV KI-SYSTEMER som er komponenter i de store IT-systemene som er etablert ved rettsaktene oppført I et vedlegg til denne forordning, og operatører AV høyrisiko KI-systemer som er beregnet å brukes av offentlige myndigheter, treffe de nødvendige tiltak for å oppfylle kravene i denne forordning innen henholdsvis utgangen av 2030 og innen 2. august 2030.

(178) Leverandører AV høyrisiko-AI-systemer oppfordres til å begynne å overholde de relevante forpliktelsene i denne forordningen på frivillig basis allerede i overgangsperioden.

(179) Denne forordning bør få anvendelse fra 2. august 2026. Med tanke på den uakseptable risikoen forbundet med bruk AV AI PÅ visse måter, bør imidlertid forbudene samt de generelle bestemmelsene i denne forordning få anvendelse allerede fra 2. februar 2025. Selv om den fulle virkningen av disse forbudene følger med innføringen av styringen og håndhevingen av denne forordning, er det viktig å foregripe anvendelsen av forbudene for å ta hensyn til uakseptable risikoer og for å påvirke andre prosedyrer, f.eks. i sivilretten. Videre bør infrastrukturen knyttet til styringen og systemet for samsvarsvurdering være i drift før 2. august 2026, og derfor bør bestemmelsene om meldte organer og styringsstruktur gjelde fra 2. august 2025. Med tanke på den raske teknologiske utviklingen og innføringen av generelle , bør forpliktelsene for tilbydere av generelle aI-modeller gjelde fra 2. august 2025. Retningslinjer for god praksis bør være klare innen 2. mai 2025, slik at leverandørene kan dokumentere samsvar i tide. aI-kontoret bør sørge for at klassifiseringsreglene og -prosedyrene er oppdaterte i lys av den teknologiske utviklingen. I tillegg bør medlemsstatfastsette og underrette Kommisjonen om reglene for sanksjoner, herunder administrative bøter, og sikre at de gjennomføres på en korrekt og effektiv måte innen denne forordnings anvendelsesdato. Bestemmelsene om sanksjoner bør derfor få anvendelse fra 2. august 2025.

(180) Det europeiske DATATILSYNET og Det europeiske personvernrådet ble konsultert i samsvar med artikkel 42 nr. 1 og 2 i forordning (EU) 2018/1725 og avga sin felles uttalelse 18. juni 2021,

har VEDTATT denne FORSKRIFTEN:

CHaPTER I

GENERELLE BESTEMMELSER

Artikkel 1

Fagstoff

1. Formålet med denne forordningen er å forbedre det indre markedets virkemåte og fremme innføringen av menneskesentrert og pålitelig kunstig intelligens (AI), samtidig som det sikres et høyt nivå av beskyttelse av helse, sikkerhet, grunnleggende rettigheter nedfelt i pakten, herunder demokrati, rettsstatsprinsipper og miljøvern, mot de skadelige virkningene AV aI-systemer i Unionen, og å støtte innovasjon.

2. Denne forordningen fastsetter:

(a) harmoniserte regler for markedsføring, ibruktaking og bruk AV AI-systemer i Unionen;

(b) forbud mot visse former for praksis;

(c) spesifikke krav til høyrisikosystemer og forpliktelser for operatører av slike systemer;

(d) harmoniserte regler for gjennomsiktighet for visse AI-systemer;

(e) harmoniserte regler for markedsføring av allsidige AI-modeller;

(f) regler om markedsovervåking, markedsovervåking, styring og håndheving;

(g) tiltak for å støtte innovasjon, med særlig fokus på små og mellomstore bedrifter, inkludert oppstartsbedrifter.

Artikkel 2

Omfang

1. Denne forordning gjelder :

(a) tilbydere som bringer I omsetning eller tar i bruk aI-systemer ELLER BRINGER I OMSETNING aI-modeller til allmenn bruk I Unionen, uavhengig av om disse tilbyderne er etablert eller befinner seg i Unionen eller i en tredjestat;

(b) utplasserere AV AI-systemer som har sitt etableringssted eller befinner seg i Unionen;

(c) tilbydere og distributører AV aI-systemer som har sitt etableringssted eller er lokalisert i et tredjeland, der utdataene som produseres AV aI-systemet brukes i Unionen;

(d) importører og distributører AV AI-systemer;

(e) produktprodusenter som markedsfører eller tar i bruk et AI-system sammen med sitt produkt og under sitt eget navn eller varemerke;

(f) autoriserte representanter for leverandører som ikke er etablert i Unionen;

(g) berørte personer som befinner seg i Unionen.

2. For KI-systemer som er klassifisert som høyrisiko KI-SYSTEMER i samsvar med artikkel 6 nr. 1, knyttet produkter som omfattes av Unionens harmoniseringslovgivning oppført i del B i vedlegg I, bare artikkel 6 nr. 1, artikkel 102-109 og artikkel 112. Artikkel 57 gjelder bare I den grad kravene til høyrisiko KI-systemer i henhold til denne forordning er integrert i Unionens harmoniseringslovgivning.

3. Denne forordning får ikke anvendelse på områder som faller utenfor unionsrettens virkeområde, og skal under enhver omstendighet ikke berøre medlemsstatenes myndighet når det gjelder nasjonal sikkerhet, uavhengig hvilken type enhet som av har fått i oppdrag å utføre oppgaver i forbindelse med denne myndighet.

Denne forordning får ikke anvendelse på AI-systemer når og i den grad de bringes omsetning, tas i bruk eller brukes med eller uten endringer utelukkende for militære formål, forsvarsformål eller nasjonale sikkerhetsformål, uavhengig av hvilken type enhet som utfører disse aktivitetene.

Denne forordning får ikke anvendelse på AI-systemer som ikke er brakt i omsetning eller tatt i bruk i Unionen, dersom produktene utelukkende brukes i Unionen til militære formål, forsvarsformål eller nasjonale sikkerhetsformål, uavhengig av hvilken type enhet som utfører disse aktivitetene.

4. Denne forordning får verken anvendelse på offentlige myndigheter i en tredjestat eller på internasjonale organisasjoner som omfattes av denne forordnings virkeområde I henhold til nr. 1, dersom disse myndighetene eller organisasjonene bruker innenfor rammen av internasjonalt samarbeid eller avtaler om rettshåndheving og rettslig samarbeid med Unionen eller med en eller flere medlemsstater, forutsatt at tredjestaten eller den internasjonale organisasjonen gir tilstrekkelige garantier med hensyn til vern av fysiske personers grunnleggende rettigheter og friheter.

5. Denne forordning skal ikke berøre anvendelsen av bestemmelsene om erstatningsansvar for ytere av formidlingstjenester som fastsatt i kapittel II i forordning (EU) 2022/2065.

6. Denne forordning får ikke anvendelse på KI-systemer eller KI-modeller, herunder deres resultater, som er spesielt utviklet og i bruk utelukkende med det formål å drive vitenskapelig forskning og utvikling.

7. Unionsretten om vern av personopplysninger, personvern og kommunikasjonshemmeligheter får anvendelse på personopplysninger som behandles i forbindelse med rettighetene og pliktene fastsatt i denne forordning. Denne forordning skal ikke berøre forordning (EU) 2016/679 eller (EU) 2018/1725, eller direktiv 2002/58/EF eller (EU) 2016/680, med forbehold for artikkel 10 nr. 5 og artikkel 59 i denne forordning.

8. Denne forordning får ikke anvendelse på forskning, prøving eller utvikling av KI-systemer ELLER KI-modeller før de bringes i omsetning eller tas i bruk. Slike aktiviteter skal utføres i samsvar med gjeldende unionsrett. Testing under reelle forhold skal ikke omfattes av dette unntaket.

9. Denne forordning berører ikke reglene som er fastsatt i andre unionsrettsakter om forbrukerbeskyttelse og produktsikkerhet.

10. Denne forordningen gjelder ikke for forpliktelser for som er fysiske personer som bruker AI-systemer i forbindelse med en rent personlig, ikke-profesjonell aktivitet.

11. Denne forordning er ikke til hinder for at Unionen eller medlemsstatene opprettholder eller innfører lover og forskrifter som er gunstigere for arbeidstakerne når det gjelder vern AV deres rettigheter I forbindelse med arbeidsgiveres bruk AV AI-systemer, eller at de oppmuntrer til eller tillater anvendelse av tariffavtaler som ER gunstigere for arbeidstakerne.

12. Denne forordning får ikke anvendelse på aI-systemer som er utgitt under lisenser med fri og åpen kildekode, med mindre de bringes i omsetning eller tas i bruk som høyrisikosystemer eller som et aI-system som faller inn under artikkel 5 eller 50.

Artikkel 3

Definisjoner

I denne forordning gjelder følgende definisjoner:

(1) "aI-system": et maskinbasert system som er utformet for å operere med varierende grad av autonomi, og som kan vise tilpasningsdyktighet etter utplassering, og som, for eksplisitte eller implisitte mål, utleder fra inndataene det mottar, hvordan det skal generere utdata, for eksempel spådommer, innhold, anbefalinger eller beslutninger som kan påvirke fysiske eller virtuelle miljøer;

(2) "risiko": kombinasjonen av sannsynligheten for at en skade skal inntreffe og alvorlighetsgraden av denne ;

(3) "leverandør": en fysisk eller juridisk person, offentlig myndighet, etat eller annet organ som utvikler et aI-system eller en generell aI-modell, eller som får utviklet et aI-system eller en generell aI-modell og bringer det i omsetning eller tar aI-systemet i bruk under eget navn eller varemerke, enten mot betaling eller vederlagsfritt;

(4) "utplasserende enhet": en fysisk eller juridisk person, offentlig myndighet, etat eller annet organ som bruker et KI-system under sin myndighet, unntatt der KI-SYSTEMET brukes i forbindelse med en personlig, ikke-profesjonell aktivitet;

(5) "autorisert representant" en fysisk eller juridisk person som befinner seg eller er etablert i Unionen, og som har mottatt og akseptert en skriftlig fullmakt fra en leverandør av et AI-system eller en generell AI-modell til henholdsvis å oppfylle og utføre på dennes vegne de forpliktelser og framgangsmåter som er fastsatt i denne forordning;

(6) "importør" en fysisk eller juridisk person som befinner seg eller er etablert i Unionen, OG SOM BRINGER I OMSETNING ET AI-system som bærer navnet eller varemerket til en fysisk eller juridisk person som er etablert i en tredjestat;

(7) "distributør": en fysisk eller juridisk person i forsyningskjeden, bortsett fra leverandøren eller importøren, som gjør et AI-system tilgjengelig på unionsmarkedet;

(8) "operatør": en leverandør, produktprodusent, distributør, autorisert representant, importør eller distributør;

(9) "bringe I omsetning": første gangs tilgjengeliggjøring av et AI-system eller EN AI-modell for allmenn bruk på unionsmarkedet;

(10) "gjøre tilgjengelig på markedet": levering av et AI-system eller EN AI-modell til allmenn bruk for distribusjon eller bruk på unionsmarkedet som ledd i næringsvirksomhet, enten mot betaling eller vederlagsfritt;

(11) "IBRUKTAKING": levering av et AI-system for første gangs bruk direkte til den som utplasserer det, eller for eget bruk i Unionen til det tiltenkte formål;

(12) "tiltenkt formål": den bruken som leverandøren har tiltenkt et KI-system, herunder den spesifikke konteksten og de spesifikke bruksbetingelsene, som spesifisert i informasjonen leverandøren har gitt i bruksanvisninger, salgsfremmende eller salgsfremmende materiale og erklæringer, samt i den tekniske dokumentasjonen;

(13) "misbruk som med rimelighet kan forutses": bruk av et KI-system på en måte som ikke er i samsvar med dets tiltenkte formål, men som kan være et resultat av menneskelig atferd eller interaksjon med andre systemer, herunder andre KI-systemer, som med rimelighet kan forutses;

(14) "sikkerhetskomponent": en komponent I et produkt eller I et luftfartssystem som oppfyller en sikkerhetsfunksjon for produktet eller LUFTFARTSSYSTEMET, eller svikt eller funksjonssvikt utgjør en fare for personers helse og sikkerhet eller for materielle verdier;

(15) "bruksanvisning": den informasjonen som leverandøren gir for å informere brukeren om, særlig, et AI-systems tiltenkte formål og korrekte bruk;

(16) "tilbakekalling av et aI-system": ethvert tiltak som tar sikte på å oppnå tilbakeføring til leverandøren eller å ta ut av drift eller deaktivere bruken av et aI-system som er gjort tilgjengelig for utplasserere;

(17) "tilbaketrekking AV et aI-system": ethvert tiltak som tar sikte på å hindre at et aI-system i forsyningskjeden gjøres tilgjengelig på markedet;

(18) "ytelsen til et KI-system": ET KI-systems evne til å oppnå sitt tiltenkte formål;

(19) "meldermyndighet": den nasjonale myndighet som er ansvarlig for å opprette og gjennomføre de nødvendige framgangsmåter for vurdering, utpeking og melding av samsvarsvurderingsorganer og for overvåking av disse;

(20) "samsvarsvurdering": prosessen for å påvise om kravene fastsatt I kapittel III, avsnitt 2 vedrørende et høyrisiko-AI-system er oppfylt;

(21) "samsvarsvurderingsorgan": et organ som utfører tredjeparts samsvarsvurderingsaktiviteter, herunder prøving, sertifisering og inspeksjon;

(22) "meldt organ": et samsvarsvurderingsorgan som er meldt i samsvar med denne forordning og annen relevant unionsharmoniseringslovgivning;

(23) "vesentlig endring": en endring av et AI-system etter at det er brakt I omsetning eller tatt i bruk, som ikke var forutsett eller planlagt i den opprinnelige samsvarsvurderingen som ble utført av leverandøren, og som medfører AI-systemets samsvar med kravene i kapittel III avsnitt 2 påvirkes eller fører til en endring av det tiltenkte formålet som AI-SYSTEMET er vurdert for;

(24) "": en merking som en leverandør bruker for å angi at et AI-system er I samsvar med kravene fastsatt i kapittel III, avsnitt 2 og annen gjeldende EU-harmoniseringslovgivning som fastsetter påføring av denne;

(25) "system for overvåking etter at utstyret er brakt i omsetning": alle aktiviteter som utføres av leverandører av KI-SYSTEMER for å samle inn og gjennomgå erfaringer fra bruken AV KI-systemer som de har brakt i omsetning eller tatt i bruk, med det formål å identifisere eventuelle behov for å iverksette nødvendige korrigerende eller forebyggende tiltak umiddelbart;

(26) "markedstilsynsmyndighet" den nasjonale myndigheten som utfører aktivitetene og treffer tiltakene i henhold til forordning (EU) 2019/1020;

(27) "harmonisert standard": en harmonisert standard som definert i artikkel 2 nr. 1 bokstav c) i forordning (EU) nr. 1025/2012;

(28) "felles spesifikasjon": et sett tekniske spesifikasjoner som definert i artikkel 2 nr. 4 i forordning (EU) nr. 1025/2012, som angir hvordan visse krav fastsatt i henhold til denne forordning kan oppfylles;

(29) "opplæringsdata": data som brukes til å lære opp ET AI-system ved å tilpasse dets lærbare parametere;

(30) "valideringsdata": data som brukes til å evaluere det opplærte AI-systemet og til å justere dets ikke-lærbare parametere og læringsprosessen, blant annet for å hindre undertilpasning eller overtilpasning;

(31) "" betyr et separat datasett eller en del av , enten som en fast eller variabel oppdeling;

(32) "testdata" data som brukes til å foreta en uavhengig evaluering AV AI-systemet for å bekrefte systemets forventede ytelse før det bringes i omsetning eller tas i bruk;

(33) "inndata" data som leveres til eller innhentes direkte AV ET AI-system, og på grunnlag av hvilke systemet produserer en utdata;

(34) "biometriske opplysninger": personopplysninger som er et resultat av spesifikk teknisk behandling knyttet til en fysisk persons fysiske, fysiologiske eller atferdsmessige kjennetegn, f.eks. ansiktsbilder eller fingeravtrykksdata;

(35) "biometrisk identifikasjon": automatisert gjenkjenning av fysiske, fysiologiske, atferdsmessige eller psykologiske menneskelige kjennetegn med det formål å fastslå identiteten til en fysisk person ved å sammenligne biometriske data om denne personen med biometriske data om enkeltpersoner som er lagret i en database;

(36) "biometrisk verifisering": automatisert én-til-én-verifisering, herunder autentisering, av fysiske personers identitet ved å sammenligne deres biometriske data med tidligere oppgitte biometriske data;

(37) "særlige kategorier av personopplysninger": de kategorier av personopplysninger som er nevnt i artikkel 9 nr. 1 i forordning (EU) 2016/679, artikkel 10 i direktiv (EU) 2016/680 og artikkel 10 nr. 1 i forordning (EU) 2018/1725;

(38) "sensitive operasjonelle opplysninger": operasjonelle opplysninger knyttet til aktiviteter for å forebygge, avdekke, etterforske eller straffeforfølge straffbare handlinger, og hvis utlevering kan sette straffeforfølgningens integritet i fare;

(39) "" et KI-system som HAR til formål å identifisere eller utlede følelser eller intensjoner hos fysiske personer på grunnlag av deres biometriske data;

(40) "biometrisk kategoriseringssystem" et AI-SYSTEM som har til formål å tilordne fysiske personer til bestemte kategorier på grunnlag av deres biometriske data, med mindre det er tilknyttet en annen kommersiell tjeneste og er strengt nødvendig av objektive tekniske grunner;

(41) "fjernstyrt biometrisk identifikasjonssystem"ET AI-system identifisering AV fysiske personer, uten deres aktive medvirkning, vanligvis på avstand gjennom sammenligning av en persons biometriske data med de biometriske dataene i en referansedatabase;

(42) "system for fjernstyrt biometrisk identifikasjon i sanntid": et system for fjernstyrt biometrisk identifikasjon, der opptaket av biometriske data, sammenligningen og identifikasjonen skjer uten vesentlig forsinkelse, og som ikke bare omfatter umiddelbar identifikasjon, men også begrensede korte forsinkelser for å unngå omgåelse;

(43) "system for biometrisk identifikasjon etter fjernidentifikasjon": et system for biometrisk fjernidentifikasjon enn et system for biometrisk fjernidentifikasjon i sanntid;

(44) "offentlig tilgjengelig sted": ethvert offentlig eller privateid fysisk sted som er tilgjengelig for et ubestemt antall fysiske personer, uavhengig av om det gjelder visse vilkår for tilgang, og uavhengig av eventuelle kapasitetsbegrensninger;

(45) "rettshåndhevende myndighet" betyr:

(a) enhver offentlig myndighet som har kompetanse til å forebygge, etterforske, avsløre eller straffeforfølge straffbare handlinger eller fullbyrde strafferettslige sanksjoner, herunder å beskytte mot og forebygge trusler mot den offentlige sikkerhet; eller

(b) ethvert annet organ eller enhver annen enhet som i henhold til medlemsstatens lovgivning er betrodd å utøve offentlig myndighet og offentlig makt for å forebygge, etterforske, avsløre eller straffeforfølge straffbare handlinger eller fullbyrde strafferettslige sanksjoner, herunder å beskytte mot og forebygge trusler mot den offentlige sikkerhet;

(46) "rettshåndhevelse" aktiviteter som utføres av rettshåndhevende myndigheter eller på deres vegne for å forebygge, etterforske, avsløre eller straffeforfølge straffbare handlinger eller fullbyrde strafferettslige sanksjoner, herunder å beskytte mot og forebygge trusler mot den offentlige sikkerhet;

(47) "aI-kontoret" Kommisjonens funksjon med å bidra til gjennomføring, overvåking og tilsyn med aI-systemer og generelle aI-modeller og aI-forvaltning, fastsatt i Kommisjonens beslutning av 24. januar 2024; henvisninger i denne forordning til aI-kontoret skal forstås som henvisninger til Kommisjonen;

(48) "nasjonal vedkommende myndighet": varslingsmyndighet eller ; når det gjelder AI-systemer som er tatt i bruk eller brukes av Unionens institusjoner, byråer, kontorer og organer, skal henvisninger til nasjonale vedkommende myndigheter eller markedstilsynsmyndigheter i denne forordning forstås som henvisninger til Den europeiske datatilsynsmann;

(49) "alvorlig hendelse": en hendelse eller funksjonssvikt I ET AI-system som direkte eller indirekte fører til noe av det følgende:

(a) en persons død, eller alvorlig skade på en persons helse;

(b) en alvorlig og irreversibel forstyrrelse av styringen eller driften av kritisk infrastruktur;

(c) brudd på unionsrettslige forpliktelser som har til formål å beskytte grunnleggende rettigheter;

(d) alvorlig skade på eiendom eller miljø;

(50) "personopplysninger" betyr personopplysninger som definert i artikkel 4 nr. 1 i forordning (EU) 2016/679;

(51) "ikke-personlige opplysninger" betyr andre opplysninger enn personopplysninger som definert i artikkel 4 nr. 1 i forordning (EU) 2016/679;

(52) "profilering" betyr profilering som definert i artikkel 4 nr. 4 i forordning (EU) 2016/679;

(53) "plan for utprøving i den virkelige verden": et dokument som beskriver mål, metodikk, geografisk, populasjonsmessig og tidsmessig omfang, overvåking, organisering og gjennomføring av utprøving under virkelige forhold;

(54) "sandkasseplan": et dokument som er avtalt mellom den deltakende leverandøren og vedkommende myndighet, og som beskriver mål, vilkår, tidsramme, metodikk og krav for aktivitetene som utføres i sandkassen;

(55) "regulatorisk sandkasse FOR AI": et kontrollert rammeverk som er opprettet av en vedkommende myndighet, og som gir tilbydere eller potensielle tilbydere av aI-systemer mulighet til å utvikle, lære opp, validere og teste, eventuelt under reelle forhold, et innovativt aI-system i henhold til en sandkasseplan i en begrenset periode under myndighetstilsyn;

(56) "aI-kompetanse": ferdigheter, kunnskaper og forståelse som gjør det mulig for leverandører, brukere og berørte personer, under hensyntagen til deres respektive rettigheter og plikter i henhold til denne forordning, å ta i bruk aI-systemer PÅ et informert grunnlag, samt å bli bevisst på mulighetene og risikoene ved AI og mulige skader det kan forårsake;

(57) "prøving under reelle forhold": midlertidig prøving av et KI-system for dets tiltenkte formål under reelle forhold utenfor et laboratorium eller et på annen måte simulert miljø, med sikte på å samle inn pålitelige og robuste data og vurdere og verifisere KI-SYSTEMETS samsvar med kravene i denne forordning, og det kvalifiserer ikke til å bringe KI-SYSTEMET i omsetning eller ta det i bruk i henhold til denne forordning, forutsatt at alle vilkårene fastsatt i artikkel 57 eller 60 er oppfylt;

(58) "forsøksperson": en fysisk person som deltar i testing under virkelige forhold;

(59) "informert samtykke": en forsøkspersons frivillige, spesifikke, entydige og frivillige uttrykk for at han eller hun er villig til å delta i en bestemt testing under reelle forhold, etter å ha blitt informert om alle aspekter ved testingen som er relevante for forsøkspersonens beslutning om å delta;

(60) "dyp forfalskning": ET I-genererte eller manipulert bilde, lyd- eller videoinnhold som ligner på eksisterende personer, gjenstander, steder, enheter eller hendelser, og som feilaktig kan fremstå som autentisk eller sannferdig for en person;

(61) "utbredt overtredelse": enhver handling eller unnlatelse som er i strid med unionsretten som beskytter enkeltpersoners interesser, og som:

(a) har skadet eller sannsynligvis vil skade de kollektive interessene til enkeltpersoner som er bosatt i minst to andre medlemsstater enn den medlemsstaten der:

(i) handlingen eller unnlatelsen oppsto eller fant sted;

(ii) den berørte leverandøren, eller dennes autoriserte representant, befinner seg eller er etablert; eller

(iii) utleverer er etablert, når overtredelsen er begått av utleverer;

(b) har forårsaket, forårsaker eller sannsynligvis vil forårsake skade på enkeltpersoners kollektive interesser og har fellestrekk, herunder samme ulovlige praksis eller samme interesse som krenkes, og forekommer samtidig, begått av samme aktør, i minst tre medlemsstater;

(62) "kritisk infrastruktur" kritisk infrastruktur som definert i artikkel 2 nr. 4 i direktiv (EU) 2022/2557;

(63) "generell KI-modell" en KI-modell, herunder når en slik KI-modell er opplært med en stor data ved hjelp av selvovervåking i stor skala, som viser betydelig generalitet og er i stand til å utføre et bredt spekter av distinkte oppgaver på EN kompetent måte, uavhengig av hvordan modellen markedsføres, og som kan integreres i en rekke nedstrømssystemer eller -applikasjoner, med unntak av KI-MODELLER som brukes til forskning, utvikling eller prototyping før de markedsføres;

(64) "kapasiteter med stor gjennomslagskraft" betyr kapasiteter som tilsvarer eller overgår de kapasitetene som er registrert i de mest avanserte AI-modellene for generelle formål;

(65) "systemrisiko": en risiko som er spesifikk for de allmenne KI-modellenes evner til å ha stor innvirkning, og som har en betydelig innvirkning på unionsmarkedet på grunn av deres rekkevidde, eller på grunn av faktiske eller rimelig forutsigbare negative virkninger på folkehelsen, sikkerheten, den offentlige tryggheten, grunnleggende rettigheter eller samfunnet som helhet, og som kan forplante seg i stor skala gjennom hele verdikjeden;

(66) "allsidig aI-system": et AI-SYSTEM som er basert på en allsidig aI-modell, og som kan brukes til en rekke formål, både til direkte bruk og til integrering i andre aI-systemer;

(67) "Flytekomma-operasjon": enhver matematisk operasjon eller oppgave som involverer flytekommatall, som er en delmengde av de reelle tallene som vanligvis representeres på datamaskiner av et heltall med fast presisjon skalert med en heltallseksponent med fast base;

(68) "nedstrømsleverandør": en leverandør av et aI-system, herunder et generelt aI-system, som integrerer en aI-modell, uavhengig av om aI-modellen leveres av dem selv og er vertikalt integrert eller leveres av en annen enhet på grunnlag av kontraktsforhold.

Artikkel 4

AI-kompetanse

Tilbydere og ibruktakere AV KI-systemer skal treffe tiltak for å sikre, så langt det er mulig, at deres ansatte og andre personer som arbeider med drift og bruk av KI-SYSTEMER på deres vegne, har tilstrekkelige KI-kunnskaper, idet det tas hensyn til deres tekniske kunnskaper, erfaring, utdanning og opplæring og den sammenhengen KI-systemene skal brukes i, og idet det tas hensyn til de personer eller grupper av personer som KI-systemene skal brukes på.

CHaPTER II

FORBUDT AI-PRAKSIS

Artikkel 5

Forbudt AI-praksis

1. Følgende praksis skal være forbudt:

(a) markedsføring, ibruktaking eller bruk av et AI-system som benytter subliminale teknikker utenfor en persons bevissthet eller bevisst manipulerende eller villedende teknikker, med det formål eller den virkning å vesentlig forvrenge atferden til en person eller en gruppe personer ved I betydelig grad å svekke deres evne til å treffe en informert beslutning, og derved få dem til å treffe en beslutning som de ellers ikke ville ha truffet, på en måte som volder eller med rimelig sannsynlighet vil volde denne personen, en annen person eller en gruppe av personer betydelig skade;

(b) markedsføring, ibruktaking eller bruk av ET AI-system som utnytter sårbarheten til en fysisk person eller en bestemt gruppe personer på grunn av alder, funksjonshemming eller en bestemt sosial eller økonomisk situasjon, med det formål eller den virkning å vesentlig forvrenge atferden til denne personen eller en person som tilhører denne gruppen, på en måte som forårsaker eller med rimelig sannsynlighet vil forårsake betydelig skade for denne personen eller en annen ;

(c) markedsføring, ibruktaking eller bruk AV AI-systemer for evaluering eller klassifisering av fysiske personer eller grupper av personer over en viss tidsperiode på grunnlag av deres sosiale atferd eller kjente, utledede eller forventede personlige eller personlighetsmessige egenskaper, der den sosiale poengsummen fører til en eller begge av følgende

(i) ufordelaktig eller ugunstig behandling av visse fysiske personer eller grupper av personer i sosiale sammenhenger som ikke er relatert til de sammenhengene der opplysningene opprinnelig ble generert eller samlet inn;

(ii) ufordelaktig eller ugunstig behandling av visse fysiske personer eller grupper av personer som er uberettiget eller uforholdsmessig i forhold til deres sosiale atferd eller dens alvorlighetsgrad;

(d) markedsføring, ibruktaking for dette spesifikke formålet eller bruk av ET KI-system for å foreta risikovurderinger av fysiske personer for å vurdere eller forutsi risikoen for at en fysisk person begår en straffbar handling, utelukkende basert på profilering av en fysisk person eller på vurdering av vedkommendes personlighetstrekk og egenskaper; dette forbudet får ikke anvendelse på KI-systemer som brukes til å støtte den menneskelige vurderingen av en persons involvering i en kriminell aktivitet, som allerede er basert på objektive og verifiserbare fakta som er direkte knyttet til en kriminell aktivitet;

(e) markedsføring, ibruktaking for dette spesifikke formålet, eller bruk AV KI-systemer som oppretter eller utvider ansiktsgjenkjenningsdatabaser ved hjelp av ikke-målrettet skraping av ansiktsbilder fra internett eller overvåkningsopptak;

(f) markedsføring, ibruktaking for dette spesifikke formålet, eller bruk AV aI-systemer for å utlede følelser hos en fysisk person på arbeidsplassen og i utdanningsinstitusjoner, unntatt når bruken AV AI-SYSTEMET er ment å bli satt på plass eller markedsført av medisinske eller sikkerhetsmessige årsaker;

(g) markedsføring, ibruktaking for dette spesifikke formålet eller bruk av biometriske kategoriseringssystemer som kategoriserer individuelle fysiske personer på grunnlag av deres biometriske data for å utlede eller slutte seg til deres rase, politiske meninger, fagforeningsmedlemskap, religiøse eller filosofiske overbevisning, seksualliv eller seksuelle legning; dette forbudet omfatter ikke merking eller filtrering av lovlig ervervede biometriske datasett, f.eks. bilder, på grunnlag av biometriske data eller kategorisering av biometriske data på rettshåndhevingsområdet;

(h) bruk av fjernstyrte biometriske identifikasjonssystemer i "sanntid" på offentlig tilgjengelige steder med henblikk på rettshåndhevelse, med mindre og i den grad slik bruk er strengt nødvendig for ett av følgende formål

(i) målrettet leting etter spesifikke ofre for bortføring, menneskehandel eller seksuell utnyttelse av , samt leting etter savnede personer;

(ii) avverging av en konkret, vesentlig og overhengende trussel mot fysiske personers liv eller fysiske sikkerhet eller en reell og aktuell eller reell og forutsigbar trussel om et terrorangrep;

(iii) lokalisering eller identifisering av en person som mistenkes for ha begått en straffbar handling, med henblikk på å gjennomføre en strafferettslig etterforskning eller straffeforfølgning eller fullbyrde en strafferettslig reaksjon for lovbrudd som er nevnt i vedlegg II, og som i den berørte medlemsstaten kan straffes med en frihetsstraff eller en frihetsberøvende reaksjon med en maksimumsperiode på minst fire år.

Første ledd bokstav h) berører ikke artikkel 9 i forordning (EU) 2016/679 for behandling av biometriske opplysninger for andre formål enn rettshåndheving.

2. Bruk av systemer for fjernstyrt biometrisk identifikasjon i "sanntid" på offentlig tilgjengelige steder med henblikk på rettshåndheving for noen av formålene nevnt i nr. 1 første ledd bokstav h), skal bare brukes for formålene nevnt i nevnte bokstav for å bekrefte identiteten til den personen som er spesifikt utpekt som mål, og det skal tas hensyn til følgende elementer:

(a) arten av situasjonen som ligger til grunn for den mulige bruken, særlig alvoret, sannsynligheten og omfanget av den skaden som ville oppstå dersom systemet ikke ble brukt;

(b) konsekvensene av bruken av systemet for alle berørte personers rettigheter og friheter, særlig alvoret, sannsynligheten for og omfanget av disse konsekvensene.

I tillegg skal bruken av systemer for fjernstyrt biometrisk identifikasjon i sanntid offentlig tilgjengelige steder med henblikk på rettshåndhevelse for et av målene nevnt i nr. 1 første ledd bokstav h) i denne artikkel i samsvar med nødvendige og forholdsmessige garantier og vilkår bruken i samsvar med nasjonal lovgivning som tillater bruken, særlig med hensyn til de tidsmessige, geografiske og personlige begrensningene. Bruk av systemet for fjernstyrt biometrisk identifikasjon i sanntid på offentlig tilgjengelige steder skal bare tillates dersom rettshåndhevelsesmyndigheten har gjennomført en konsekvensanalyse av de grunnleggende rettighetene som fastsatt i artikkel 27, og har registrert systemet i EU-databasen i henhold til artikkel 49. I behørig begrunnede hastetilfeller kan imidlertid bruken av slike systemer påbegynnes uten registrering i EU-databasen, forutsatt at slik registrering fullføres uten unødig forsinkelse.

3. Med henblikk på nr. 1 første ledd bokstav h) og nr. 2 skal enhver bruk av et system for fjernstyrt biometrisk identifikasjon i sanntid på offentlig tilgjengelige steder med henblikk på rettshåndhevelse være underlagt en forhåndstillatelse gitt av en rettslig myndighet eller en uavhengig forvaltningsmyndighet hvis avgjørelse er bindende for den medlemsstat der bruken skal finne sted, utstedt etter en begrunnet anmodning og i samsvar med de nærmere bestemmelsene i nasjonal rett nevnt i nr. 5. I en behørig begrunnet hastesituasjon kan imidlertid bruken av et slikt system påbegynnes uten tillatelse, forutsatt at det anmodes om slik tillatelse uten unødig opphold og senest innen 24 timer. Dersom en slik tillatelse avslås, skal bruken stanses med umiddelbar virkning, og alle data resultater og output fra denne bruken skal umiddelbart kasseres og slettes.

Den kompetente rettslige myndighet eller en uavhengig forvaltningsmyndighet hvis avgjørelse er bindende, skal bare gi tillatelse dersom den på grunnlag av objektive bevis eller klare indikasjoner som fremlegges for den, er overbevist om at bruken av det aktuelle biometriske fjernidentifikasjonssystemet i sanntid er nødvendig for, og står i et rimelig forhold til, å oppnå en av følgende

formålene angitt i nr. 1 første ledd bokstav h), slik de er angitt i anmodningen, og skal særlig begrenses til det som er strengt nødvendig med hensyn til tidsperiode samt geografisk og personlig omfang. Ved avgjørelsen av anmodningen skal nevnte myndighet ta hensyn til momentene nevnt i nr. 2. Ingen beslutning som har negative rettsvirkninger for en person, kan treffes utelukkende på grunnlag av resultatene fra systemet for biometrisk fjernidentifikasjon i sanntid.

4. Uten at det berører nr. 3, skal enhver bruk av et system for fjernstyrt biometrisk identifikasjon i sanntid på offentlig tilgjengelige steder for rettshåndhevingsformål meldes til den relevante markedstilsynsmyndigheten og den nasjonale personvernmyndigheten i samsvar med de nasjonale reglene nevnt i nr. 5. Meldingen skal som et minimum inneholde informasjonen angitt i nr. 6 og skal ikke omfatte sensitive driftsopplysninger.

5. EN medlemsstat kan beslutte å gi mulighet til helt eller delvis å gi tillatelse til bruk av systemer for fjernstyrt biometrisk identifikasjon i sanntid på offentlig tilgjengelige steder med henblikk på rettshåndhevelse innenfor de grenser og på de vilkår som er nevnt i nr. 1 første ledd bokstav h) og nr. 2 og 3. Berørte medlemsstater skal i sin nasjonale lovgivning fastsette de nødvendige nærmere regler for anmodning om, utstedelse og utøvelse av, samt tilsyn og rapportering i forbindelse , tillatelsene nevnt i nr. 3. Disse reglene skal også angi med hensyn til hvilke av målene oppført i nr. 1 første ledd bokstav h), herunder hvilke av de straffbare handlingene nevnt i nr. 1 bokstav h) iii), vedkommende myndigheter kan gis tillatelse til å bruke disse systemene med henblikk på rettshåndheving. Medlemsstatene skal underrette Kommisjonen om disse reglene senest 30 dager etter at de er vedtatt. Medlemsstatene kan i samsvar med unionsretten innføre mer restriktive lover om bruk av systemer for biometrisk fjernidentifikasjon.

6. Nasjonale markedstilsynsmyndigheter og nasjonale personvernmyndigheter i medlemsstater som har fått melding om bruk av systemer for fjernstyrt biometrisk identifikasjon i "sanntid" på offentlig tilgjengelige steder for rettshåndhevingsformål i henhold til nr. 4, skal framlegge årlige rapporter om slik bruk for Kommisjonen. For dette formål skal Kommisjonen gi medlemsstatene og de nasjonale markedstilsynsmyndighetene og personvernmyndighetene en mal, herunder informasjon om antallet avgjørelser som er truffet av vedkommende rettslige myndigheter eller en uavhengig forvaltningsmyndighet hvis avgjørelse er bindende for anmodninger om tillatelse i samsvar med nr. 3, og resultatet av disse.

7. Kommisjonen skal offentliggjøre årlige rapporter om bruken av systemer for fjernstyrt biometrisk identifikasjon i sanntid på offentlig tilgjengelige steder for rettshåndhevingsformål, basert på aggregerte data i medlemsstatene på grunnlag av de årlige rapportene nevnt i nr. 6. Disse årsrapportene skal ikke omfatte sensitive operative data om de tilknyttede rettshåndhevingsaktivitetene.

8. Denne artikkel skal ikke berøre de forbud SOM gjelder når en praksis er i strid med annen unionsrett.

CHaPTER III

AI-SYSTEMER MED HØY RISIKO

AVSNITT 1

Klassifisering av AI-systemer som høyrisikosystemer

Artikkel 6

Klassifiseringsregler for AI-systemer med høy risiko

1. Uavhengig av om et AI-system bringes i omsetning eller tas i bruk uavhengig av produktene nevnt i a) og b), skal AI-systemet anses for å være høyrisikosystem dersom begge følgende vilkår er oppfylt:

(a) aI-systemet er ment å brukes som en sikkerhetskomponent i et produkt, eller aI-systemet er i seg selv et produkt, som omfattes av Unionens harmoniseringslovgivning oppført i vedlegg I;

(b) produktet hvis sikkerhetskomponent i henhold til bokstav a) er KI-SYSTEMET, eller KI-SYSTEMET i seg selv som et produkt, skal gjennomgå en tredjeparts samsvarsvurdering med sikte på å bringe produktet i omsetning eller ta det i bruk i henhold til Unionens harmoniseringslovgivning oppført i vedlegg I.

2. I tillegg til høyrisikosystemene nevnt i nr. 1, skal aI-systemene nevnt i vedlegg III anses som høyrisikosystemer.

3. Som unntak fra nr. 2 skal et KI-system nevnt i vedlegg III ikke anses som høyrisikosystem dersom det ikke utgjør en betydelig risiko for skade på fysiske personers helse, sikkerhet eller grunnleggende rettigheter, herunder ved at det ikke i vesentlig grad påvirker utfallet av beslutningsprosessen.

Første ledd får anvendelse dersom ett av følgende vilkår er oppfylt:

(a) AI-systemet er ment å utføre en snever prosessuell oppgave;

(b) aI-systemet er ment å forbedre resultatet av en tidligere utført menneskelig aktivitet;

(c) KI-systemet er ment å oppdage beslutningsmønstre eller avvik fra tidligere beslutningsmønstre og er ikke ment å erstatte eller påvirke den tidligere fullførte menneskelige vurderingen, uten en skikkelig menneskelig gjennomgang; eller

(d) aI-systemet er ment å utføre en forberedende oppgave til en vurdering som er relevant for formålene med brukstilfellene som er oppført i vedlegg III.

Uten hensyn til første ledd skal et aI-system nevnt i vedlegg III alltid anses som høyrisikosystem dersom AI-SYSTEMET utfører profilering av fysiske personer.

4. en leverandør som anser at et AI-system nevnt i vedlegg III ikke utgjør en høy risiko, skal dokumentere sin vurdering før systemet bringes i omsetning eller tas i bruk. En slik leverandør skal være underlagt fastsatt i artikkel 49 nr. 2. På anmodning fra nasjonale vedkommende myndigheter skal leverandøren framlegge dokumentasjonen for vurderingen.

5. Kommisjonen skal, etter å ha rådført seg med Det europeiske styret for kunstig intelligens ("styret"), senest 2. februar 2026 gi retningslinjer som spesifiserer den praktiske gjennomføringen av denne artikkelen i tråd med artikkel 96, sammen med en omfattende liste over praktiske eksempler på brukstilfeller AV aI-systemer som er høyrisiko og ikke høyrisiko.

6. Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 for å endre nr. 3 annet ledd i denne artikkel ved å tilføye nye vilkår til dem som er fastsatt der, eller ved å endre dem, dersom det foreligger konkrete og pålitelige bevis for AT det finnes AI-systemer som faller inn under virkeområdet til vedlegg III, men som ikke utgjør en betydelig risiko for skade på fysiske personers helse, sikkerhet eller grunnleggende rettigheter.

7. Kommisjonen skal vedta delegerte rettsakter i samsvar med artikkel 97 for å endre nr. 3 annet ledd i denne artikkel ved å oppheve noen av vilkårene som er fastsatt der, dersom det foreligger konkrete og pålitelige bevis for at dette er nødvendig for å opprettholde det vernenivået for helse, sikkerhet og grunnleggende rettigheter som fastsatt i denne forordning.

8. Enhver endring av vilkårene fastsatt i nr. 3 annet ledd som vedtas i samsvar med nr. 6 og 7 i denne artikkel, skal ikke redusere det samlede nivået for vern av helse, sikkerhet og grunnleggende rettigheter fastsatt i denne forordning, og skal sikre samsvar med de delegerte rettsaktene vedtatt i henhold til artikkel 7 nr. 1 og ta hensyn til markedsutviklingen og den teknologiske utviklingen.

Artikkel 7

Endringer i vedlegg III

1. Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 for å endre vedlegg III ved å legge til eller endre bruksområder for høyrisikosystemer FOR KUNSTIG INTELLIGENS dersom begge følgende vilkår er oppfylt:

(a) aI-systemene er beregnet på Å brukes på alle områdene som er oppført i vedlegg III;

(b) aI-systemene utgjør en risiko for skade på helse og sikkerhet, eller en negativ innvirkning på grunnleggende rettigheter, og denne risikoen eller er større enn risikoen for skade eller negativ innvirkning som utgjøres av høyrisiko aI-systemene som allerede er nevnt i vedlegg III.

2. Ved vurderingen av vilkåret i nr. 1 bokstav b) skal Kommisjonen ta hensyn til følgende kriterier:

(a) det tiltenkte formålet med AI-systemet;

(b) I hvilken grad et AI-system har blitt brukt eller sannsynligvis vil bli ;

(c) arten og mengden av data som behandles og brukes av AI-systemet, særlig om spesielle kategorier av personopplysninger behandles;

(d) I hvilken grad KI-systemet handler autonomt, og muligheten for at et menneske kan overstyre en beslutning eller anbefalinger som kan føre til potensiell skade;

(e) I hvilken grad bruken av et AI-system allerede har forårsaket skade på helse og sikkerhet, har hatt en negativ innvirkning grunnleggende rettigheter eller har gitt opphav til betydelig bekymring med hensyn til sannsynligheten for slik skade eller negativ innvirkning, som for eksempel påvist ved rapporter eller dokumenterte påstander som er sendt til nasjonale kompetente myndigheter eller ved andre rapporter, alt etter hva som er relevant;

(f) det potensielle omfanget av slik skade eller slik negativ innvirkning, særlig når det gjelder dens intensitet og dens evne til å påvirke flere personer eller til å påvirke en bestemt gruppe personer i uforholdsmessig stor grad;

(g) i hvilken grad personer som potensielt blir skadelidende eller utsettes for negative konsekvenser, er avhengige av utfallet AV ET AI-system, særlig fordi det praktiske eller juridiske årsaker ikke er rimelig mulig å velge bort dette utfallet;

(h) i hvilken grad det er en ubalanse i maktforholdet, eller om personene som potensielt skades eller utsettes for negative konsekvenser, befinner seg i en sårbar posisjon i forhold til den som tar i bruk et AI-system, særlig på grunn av status, myndighet, kunnskap, økonomiske eller sosiale forhold eller alder;

(i) I hvilken grad resultatet av et KI-system lett kan korrigeres eller reverseres, idet det tas hensyn til de tekniske løsningene som er tilgjengelige for å korrigere eller reversere det, idet resultater som har en negativ innvirkning på helse, sikkerhet eller grunnleggende rettigheter, ikke skal anses for å være lett korrigerbare eller reversible;

(j) omfanget av og sannsynligheten for fordelene ved Å TA I BRUK AI-systemet for enkeltpersoner, grupper eller samfunnet som , inkludert mulige forbedringer i produktsikkerheten;

(k) i hvilken utstrekning gjeldende unionsrett gir bestemmelser om:

(i) effektive tiltak for å avhjelpe den risiko SOM ET AI-system utgjør, med unntak av erstatningskrav;

(ii) effektive tiltak for å forebygge eller i vesentlig grad minimere disse risikoene.

3. Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 for å endre listen I vedlegg III ved å fjerne høyrisikosystemer dersom begge de følgende vilkårene er oppfylt:

(a) det berørte høyrisikosystemet ikke lenger utgjør noen vesentlig risiko for grunnleggende rettigheter, helse eller sikkerhet, idet det tas hensyn til kriteriene oppført i nr. 2;

(b) slettingen ikke reduserer det generelle beskyttelsesnivået for helse, sikkerhet og grunnleggende rettigheter i henhold til unionsretten.

AVSNITT 2

Krav til AI-systemer med høy risiko

Artikkel 8

Overholdelse av kravene

1. KI-systemer med høy risiko skal oppfylle kravene fastsatt i denne , idet det tas hensyn til deres tiltenkte formål samt den allment anerkjente teknologiske utviklingen innen KI og KI-RELATERT teknologi. Det skal tas hensyn til risikohåndteringssystemet nevnt i artikkel 9 når det sikres at disse kravene overholdes.

2. Dersom et produkt inneholder et aI-system som omfattes av kravene i denne forordning samt kravene i Unionens harmoniseringsregelverk oppført i avsnitt A i vedlegg I, skal tilbyderne være ansvarlige for å sikre at deres produkt er I fullt samsvar med alle gjeldende krav i henhold til Unionens gjeldende . For å sikre AT høyrisiko-AI-systemene nevnt i nr. 1 er I samsvar med kravene fastsatt i dette avsnitt, og for å sikre konsekvens, unngå dobbeltarbeid og minimere tilleggsbyrder, skal leverandørene kunne velge å integrere, alt etter hva som er hensiktsmessig, de nødvendige test- og rapporteringsprosessene, opplysningene og dokumentasjonen de framlegger med hensyn til sitt produkt, i dokumentasjon og framgangsmåter som allerede finnes og kreves i henhold til Unionens harmoniseringsregelverk oppført i avsnitt A i vedlegg I.

Artikkel 9

Risikostyringssystem

1. ET risikostyringssystem skal etableres, implementeres, dokumenteres og vedlikeholdes I forbindelse med høyrisikosystemer.

2. Risikostyringssystemet skal forstås som en kontinuerlig iterativ prosess som planlegges og gjennomføres gjennom hele livssyklusen til et høyrisikosystem, og som krever regelmessig systematisk gjennomgang og oppdatering. Det skal omfatte følgende trinn:

(a) identifisering og analyse av de kjente og rimelig forutsigbare risikoene som høyrisiko-AI-systemet kan utgjøre for helse, sikkerhet eller grunnleggende rettigheter når høyrisiko-AI-systemet brukes i samsvar med sitt tiltenkte formål;

(b) estimering og evaluering av risikoene som kan oppstå når høyrisiko-AI-systemet brukes I samsvar med det tiltenkte formålet, og under forhold som med rimelighet kan forutses å være feil bruk;

(c) evaluering av andre risikoer som kan oppstå, basert på analyse av data som er samlet inn fra systemet for overvåking etter at utstyret er brakt i omsetning, jf. artikkel 72;

(d) vedta hensiktsmessige og målrettede risikostyringstiltak for å håndtere risikoene som er identifisert i henhold til bokstav a).

3. De risikoene som er nevnt i denne artikkelen, skal bare gjelde risikoer som med rimelighet kan reduseres eller elimineres gjennom utvikling eller utforming av høyrisiko-AI-systemet, eller ved at det gis tilstrekkelig teknisk informasjon.

4. Risikohåndteringstiltakene nevnt i nr. 2 bokstav d) skal ta behørig hensyn til virkningene av og den mulige samvirkningen som følger av den kombinerte anvendelsen av kravene fastsatt i dette avsnitt, med sikte på å minimere risikoene mer effektivt og samtidig oppnå en hensiktsmessig balanse i gjennomføringen av tiltakene for å oppfylle disse kravene.

5. Risikohåndteringstiltakene nevnt i nr. 2 bokstav d) skal være slik at den relevante restrisikoen knyttet til hver fare, samt den samlede restrisikoen for høyrisikosystemene, anses å være akseptabel.

Ved identifisering av de mest hensiktsmessige risikohåndteringstiltakene skal følgende sikres:

(a) eliminering eller reduksjon av risikoer som er identifisert og evaluert I henhold til nr. 2, så langt det er teknisk mulig, gjennom ADEKVAT utforming og utvikling av høyrisikosystemet;

(b) der det er hensiktsmessig, implementering av tilstrekkelige risikoreduserende og kontrollerende tiltak for å håndtere risikoer som ikke kan elimineres;

(c) formidling av informasjon som kreves i henhold til artikkel 13 og, der det er hensiktsmessig, opplæring av utplasseringspersonell.

Med sikte på å eliminere eller redusere risikoer knyttet til bruken AV høyrisiko-AI-systemet, skal det behørig hensyn til den tekniske kunnskapen, erfaringen, utdanningen og opplæringen som kan forventes av den som skal ta systemet i bruk, og den antatte sammenhengen systemet er ment å brukes i.

6. Høyrisiko aI-systemer skal testes med det formål å identifisere de mest hensiktsmessige og målrettede risikohåndteringstiltakene. Testingen skal sikre at høyrisiko-AI-systemene fungerer etter hensikten og at de er i samsvar med kravene i dette kapittelet.

7. Testprosedyrene kan omfatte testing under virkelige forhold i samsvar med artikkel 60.

8. Testing AV HØYRISIKO-AI-SYSTEMER skal utføres når som helst i løpet av utviklingsprosessen, og under alle omstendigheter før de markedsføres eller tas i bruk. Testingen skal utføres i forhold til forhåndsdefinerte måleparametere og sannsynlighetsterskler som er tilpasset formålet med .

9. Ved gjennomføringen av risikostyringssystemet som fastsatt i nr. 1 til 7, skal tjenesteytere vurdere om høyrisikosystemet I lys av sitt tiltenkte formål sannsynligvis vil ha en negativ innvirkning på personer under 18 år og, der det er relevant, andre sårbare grupper.

10. For leverandører AV høyrisiko-AI-systemer som er underlagt krav til interne risikostyringsprosesser i henhold til andre relevante bestemmelser i unionsretten, kan aspektene I nr. 1 til 9 være en del av eller kombineres med risikostyringsprosedyrene som er etablert i henhold til denne lovgivningen.

Artikkel 10

Data og datastyring

1. Høyrisiko KI-systemer som benytter teknikker som omfatter opplæring AV KI-modeller med data, skal utvikles på grunnlag av opplærings-, valideringss- og testdatasett som oppfyller kvalitetskriteriene nevnt i nr. 2-5, når slike datasett brukes.

2. Datasett for opplæring, validering og testing skal være underlagt datastyrings- og datahåndteringspraksiser som er tilpasset det tiltenkte formålet med høyrisiko-AI-systemet. Denne praksisen skal særlig omfatte følgende

(a) de relevante designvalgene;

(b) datainnsamlingsprosesser og dataenes opprinnelse, og når det gjelder personopplysninger, det opprinnelige formålet med datainnsamlingen;

(c) relevante databehandlingsoperasjoner, for eksempel annotering, merking, rensing, oppdatering, berikelse og aggregering;

(d) formulering av forutsetninger, med hensyn til informasjonen som dataene skal måle og representere;

(e) en vurdering av tilgjengeligheten, mengden og egnetheten til datasettene som trengs;

(f) undersøkelse med tanke på mulige skjevheter som kan påvirke personers helse og sikkerhet, ha en negativ innvirkning på grunnleggende rettigheter eller føre til diskriminering som er forbudt i henhold til unionsretten, særlig der datautdata påvirker input til fremtidige operasjoner;

(g) egnede tiltak for å oppdage, forebygge og redusere mulige skjevheter som er identifisert i henhold til bokstav f);

(h) identifisering av relevante datahull eller -mangler som hindrer samsvar med denne forordningen, og hvordan disse hullene og manglene kan utbedres.

3. Opplærings-, valideringss- og testdatasettene skal være relevante, tilstrekkelig representative og størst mulig grad feilfrie og fullstendige med tanke på det tiltenkte formålet. De skal ha egnede statistiske egenskaper, herunder, der det er relevant, med hensyn til de personer eller grupper av personer som høyrisikoanalysesystemet er ment å brukes i forhold til. Disse egenskapene ved datasettene kan oppfylles på nivået for de enkelte datasettene eller på nivået for en kombinasjon av disse.

4. datasettene skal, i den utstrekning det tiltenkte formålet krever det, ta hensyn til egenskaper eller elementer som er særegne for de spesifikke geografiske, kontekstuelle, atferdsmessige eller funksjonelle omgivelsene der høyrisiko-AI-systemet er ment å brukes.

5. I den utstrekning det er strengt nødvendig for å sikre oppdagelse og korrigering av skjevheter i forbindelse med høyrisiko-AI-systemene I samsvar med . 2 bokstav f) og g) I denne artikkel, kan leverandørene av slike systemer unntaksvis behandle særlige kategorier av personopplysninger, med forbehold om egnede garantier for fysiske personers grunnleggende rettigheter og friheter. I tillegg til bestemmelsene i forordning (EU) 2016/679 og (EU) 2018/1725 og direktiv (EU) 2016/680, må alle følgende vilkår være oppfylt for at slik behandling skal kunne skje:

(a) kan ikke påvisning og korrigering av skjevheter oppfylles effektivt ved å behandle andre data, inkludert syntetiske eller anonymiserte data;

(b) de særlige kategoriene av personopplysninger er underlagt tekniske begrensninger for gjenbruk av personopplysningene, og toppmoderne sikkerhets- og personverntiltak, inkludert pseudonymisering;

(c) de særlige kategoriene av personopplysninger er underlagt tiltak for å sikre at personopplysningene som behandles, er sikret, beskyttet og underlagt egnede sikkerhetstiltak, herunder streng kontroll og dokumentasjon av tilgangen, for å unngå misbruk og sikre at bare autoriserte personer har tilgang til disse personopplysningene med passende konfidensialitetsforpliktelser;

(d) de særlige kategoriene av personopplysninger skal ikke overføres, overføres eller på annen måte gjøres tilgjengelig andre parter;

(e) de spesielle kategoriene av personopplysninger slettes når er rettet eller når personopplysningene har nådd slutten av oppbevaringsperioden, avhengig av hva som kommer først;

(f) fortegnelser over behandlingsaktiviteter i henhold til forordningene (EU) 2016/679 og (EU) 2018/1725 og direktiv (EU) 2016/680 skal inneholde en begrunnelse for hvorfor behandlingen av særlige kategorier av personopplysninger var strengt nødvendig for å avdekke og korrigere skjevheter, og hvorfor dette målet ikke kunne oppnås ved å behandle andre opplysninger.

6. For utvikling av høyrisiko aI-systemer som ikke bruker teknikker som involverer opplæring AV aI-modeller, gjelder punkt 2 til 5 bare for testdatasettene.

Artikkel 11

Teknisk dokumentasjon

1. Den tekniske dokumentasjonen for et høyrisikosystem skal utarbeides før systemet bringes i omsetning eller tas i bruk, og skal holdes oppdatert.

Den tekniske dokumentasjonen skal utarbeides på en slik måte at den viser at høyrisiko-ali-systemet oppfyller kravene fastsatt i denne delen, og slik at nasjonale vedkommende myndigheter og meldte organer får de nødvendige opplysningene i en klar og utfyllende form for å kunne vurdere om aI-systemet oppfyller disse kravene. Den skal minst inneholde elementene som er angitt i vedlegg IV. Små og mellomstore bedrifter, herunder foretak, kan framlegge elementene i den tekniske dokumentasjonen angitt i vedlegg IV på en forenklet måte. For dette formål skal Kommisjonen utarbeide et forenklet skjema for teknisk dokumentasjon som er rettet mot behovene til små foretak og mikroforetak. Dersom en SMB, herunder en nystartet virksomhet, velger å framlegge opplysningene som kreves i vedlegg IV, på en forenklet måte, skal den bruke skjemaet nevnt i dette ledd. Meldte organer skal godta skjemaet i forbindelse med samsvarsvurderingen.

2. Dersom et høyrisikosystem FOR AI knyttet til et produkt som omfattes av Unionens harmoniseringsregelverk oppført i avsnitt A i vedlegg I, bringes i omsetning eller tas i bruk, skal det utarbeides ett enkelt sett med teknisk dokumentasjon som inneholder alle opplysningene fastsatt i nr. 1, samt de opplysningene som kreves i henhold til disse rettsaktene.

3. Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 for om nødvendig å endre vedlegg IV for å sikre at den tekniske dokumentasjonen, i lys av den tekniske utviklingen, gir alle opplysninger som er nødvendige for å vurdere om systemet er i samsvar med kravene fastsatt i denne avdeling.

Artikkel 12

Journalføring

1. Høyrisikosystemer skal teknisk sett muliggjøre automatisk registrering av hendelser (logger) i løpet av systemets levetid.

2. For å sikre en grad av sporbarhet AV funksjonen til ET høyrisiko-AI-system som er hensiktsmessig i forhold til systemets tiltenkte formål, skal loggingskapasiteten gjøre det mulig å registrere hendelser som er relevante for:

(a) identifisere situasjoner som kan føre til at høyrisikoalarmsystemet utgjør en risiko i henhold til artikkel 79 nr. 1, eller til en vesentlig endring;

(b) legge til rette for overvåking etter at utstyret er brakt i omsetning som nevnt i artikkel 72; og

(c) overvåking AV driften AV høyrisikosystemer som nevnt i artikkel 26 nr. 5.

3. For høyrisikosystemer som nevnt i nr. 1 bokstav a) i vedlegg III, skal loggføringskapasiteten minst omfatte følgende

(a) registrering av perioden for hver bruk av systemet (startdato og -klokkeslett og sluttdato og -klokkeslett for hver bruk);

(b) referansedatabasen som systemet har kontrollert inndataene mot;

(c) inndataene som søket har gitt treff for;

(d) identifikasjon av de fysiske personene som er involvert i verifiseringen av resultatene, som nevnt i artikkel 14 nr. 5.

Artikkel 13

Åpenhet og informasjon til distributørene

1. høyrisiko-AI-systemer skal utformes og utvikles på en slik at det sikres at driften av dem er tilstrekkelig gjennomsiktig til at driftsansvarlige kan tolke systemets resultater og bruke dem på riktig måte. en passende type og grad av gjennomsiktighet skal sikres med sikte på å oppnå samsvar med de relevante forpliktelsene til leverandøren og driftsansvarlige som er fastsatt i avsnitt 3.

2. Høyrisiko-AI-systemer skal ledsages av bruksanvisninger i et egnet digitalt format eller på annen måte som inneholder kortfattet, fullstendig, korrekt og tydelig informasjon som er relevant, tilgjengelig og forståelig for dem som bruker dem.

3. Bruksanvisningen skal minst inneholde følgende informasjon:

(a) identiteten og kontaktopplysningene til leverandøren og, der det er relevant, til dennes autoriserte representant;

(b) egenskaper, muligheter og begrensninger I ytelsen TIL høyrisiko-AI-systemet, inkludert:

(i) det tiltenkte formålet;

(ii) nøyaktighetsnivået, herunder dets beregninger, robusthet og cybersikkerhet som nevnt I artikkel 15, som høyrisiko-AI-systemet har blitt testet og validert mot, og som kan forventes, og alle kjente og forutsigbare omstendigheter som kan ha innvirkning på det forventede nøyaktighetsnivået, robustheten og cybersikkerheten;

(iii) enhver kjent eller forutsigbar omstendighet knyttet til bruken AV høyrisiko-AI-systemet i samsvar med dets tiltenkte formål eller under forhold med rimelig forutsigbar feilbruk, som kan føre til risiko for helse og sikkerhet eller grunnleggende rettigheter som nevnt i artikkel 9 nr. 2;

(iv) der det er relevant, den tekniske kapasiteten og egenskapene til høyrisiko-AI-systemet for å fremskaffe informasjon som er relevant for å forklare dets resultater;

(v) når det er hensiktsmessig, dets ytelse med hensyn til bestemte personer eller grupper av personer som systemet er ment å brukes på;

(vi) når det er hensiktsmessig, spesifikasjoner for inngangsdataene eller annen relevant informasjon om trenings-, valideringsog testdatasettene som brukes, med tanke på det tiltenkte formålet med høyrisiko-AI-systemet;

(vii) der det er relevant, informasjon som gjør det mulig for utplasseringsansvarlige å tolke utdataene fra høyrisiko-AI-systemet og bruke dem på riktig måte;

(c) eventuelle endringer I høyrisiko-AI-systemet og dets ytelse som er forhåndsbestemt av leverandøren på tidspunktet for den første samsvarsvurderingen;

(d) de menneskelige tilsynstiltakene nevnt i artikkel 14, herunder de tekniske tiltakene som er iverksatt for å gjøre det lettere for utplasseringspersonalet å tolke resultatene fra høyrisiko-AI-systemene;

(e) de nødvendige beregnings- og maskinvareressursene, forventede levetiden til høyrisiko-AI-systemet og eventuelle nødvendige vedlikeholds- og pleietiltak, herunder hyppigheten av disse, for å sikre at AI-systemet fungerer som det skal, herunder når det gjelder programvareoppdateringer;

(f) der det er relevant, en beskrivelse av mekanismene som inngår i høyrisiko-AI-systemet, og som gjør det mulig for utplasserere å samle inn, lagre og tolke loggene på riktig måte i samsvar med artikkel 12.

Artikkel 14

Menneskelig tilsyn

1. Høyrisiko-AI-systemer skal utformes og utvikles på en slik måte, blant annet ved hjelp av egnede verktøy for menneske-maskin-grensesnitt, at de effektivt kan overvåkes av fysiske personer i den perioden de er i bruk.

2. Menneskelig tilsyn skal ha som mål å forebygge eller minimere risikoene for helse, sikkerhet grunnleggende rettigheter som kan oppstå når et høyrisiko-AI-system brukes I samsvar med sitt tiltenkte formål eller under forhold med rimelig forutsigbar feilbruk, særlig når slike risikoer vedvarer til tross for anvendelsen av andre krav som er fastsatt i dette avsnittet.

3. Tilsynstiltakene skal stå i forhold til risikoene, graden av autonomi og konteksten for bruken AV høyrisiko-AI-systemet, og skal sikres gjennom enten én eller begge av følgende typer tiltak

(a) tiltak identifiseres og bygges inn i høyrisikosystemet av leverandøren, når det er teknisk mulig, før det markedsføres eller tas i bruk;

(b) tiltak som leverandøren har identifisert før høyrisikosystemet ble markedsført eller tatt i bruk, og som er hensiktsmessige å iverksette av driftsleverandøren.

4. For gjennomføringen AV nr. 1, 2 og 3 skal høyrisiko-AI-systemet stilles til rådighet for utplasseringsselskapet på en slik måte fysiske personer som er tildelt menneskelig tilsyn, aktiveres på en hensiktsmessig og forholdsmessig måte:

(a) å forstå de relevante kapasitetene og begrensningene TIL høyrisiko-AI-systemet og være i stand til å overvåke driften av det, blant annet med tanke på å avdekke og håndtere avvik, dysfunksjoner og uventede resultater;

(b) å være oppmerksom på den mulige tendensen til automatisk å stole for mye på resultatene fra et høyrisiko-AI-system (automatiseringsskjevhet), særlig FOR høyrisiko-AI-systemer som brukes til å gi informasjon eller anbefalinger for beslutninger som skal tas av fysiske personer;

(c) å tolke utdataene fra høyrisiko-AI-systemet på riktig måte, for eksempel ved å ta hensyn til tilgjengelige tolkningsverktøy og -metoder;

(d) å beslutte, i en bestemt situasjon, å ikke bruke HØYRISIKOANALYSESYSTEMET eller på annen måte se bort fra, overstyre eller reversere utdataene fra høyrisikoanalysesystemet;

(e) å gripe inn i driften AV høyrisikosystemet eller avbryte systemet ved hjelp av en "stopp"-knapp eller en lignende prosedyre som gjør det mulig å stoppe systemet i en sikker tilstand.

5. For høyrisikosystemer FOR AI som nevnt i nr. 1 bokstav a) i vedlegg III, skal tiltakene nevnt I nr. 3 i denne artikkel være slik at de I tillegg sikrer at ingen handling eller beslutning treffes av utplassøren på grunnlag av identifikasjonen som følger av systemet, med mindre denne identifikasjonen er særskilt verifisert og bekreftet av minst to fysiske personer med den nødvendige kompetanse, opplæring og myndighet.

Kravet om en separat verifisering AV minst to fysiske personer skal ikke få anvendelse PÅ høyrisiko-AI-systemer som brukes i forbindelse med rettshåndhevelse, migrasjon, grensekontroll eller asyl, dersom unionsretten eller nasjonal rett anser anvendelsen av dette kravet for å være uforholdsmessig.

Artikkel 15

Nøyaktighet, robusthet og cybersikkerhet

1. KI-systemer med høy risiko skal utformes og utvikles på en slik måte at de oppnår et passende nivå av nøyaktighet, robusthet og cybersikkerhet, og at de fungerer konsistent i disse henseendene gjennom hele livssyklusen.

2. For å håndtere de tekniske aspektene ved hvordan man skal måle de hensiktsmessige nivåene av nøyaktighet og robusthet som er fastsatt i nr. 1, og eventuelle andre relevante ytelsesmålinger, skal Kommisjonen, i samarbeid med relevante interessenter og organisasjoner, som f.eks. metrologi- og benchmarkingmyndigheter, oppmuntre til, der det er hensiktsmessig, å utvikle benchmarks og målemetoder.

3. Nøyaktighetsnivåene og de relevante nøyaktighetsmålingene FOR høyrisiko-AI-systemer skal oppgis i den medfølgende bruksanvisningen.

4. KI-systemer med høy risiko skal være så motstandsdyktige som mulig mot feil, mangler eller inkonsekvenser som kan oppstå systemet eller i det miljøet systemet opererer i, særlig på grunn av samspillet med fysiske personer eller andre systemer. Det skal treffes tekniske og organisatoriske tiltak i denne forbindelse.

Robustheten til høyrisikosystemer kan oppnås ved hjelp av tekniske redundansløsninger, som kan omfatte backup- eller fail-safe-planer.

Høyrisikosystemer FOR kunstig intelligens som fortsetter å lære etter at de er markedsført eller tatt i bruk, skal utvikles på en måte som eliminerer eller i størst mulig grad reduserer risikoen for at mulige skjeve resultater påvirker input til fremtidige operasjoner (feedback-loops), og som sikrer at slike feedback-loops blir behørig håndtert med egnede tiltak.

5. Høyrisikosystemer skal være motstandsdyktige mot forsøk fra uautoriserte tredjeparter på å endre bruken, resultatene eller ytelsen ved å utnytte sårbarheter i systemet.

De tekniske løsningene for å ivareta cybersikkerheten I høyrisiko-AI-systemer skal være tilpasset de relevante omstendighetene og risikoene.

De tekniske løsningene for å håndtere KI-spesifikke sårbarheter skal, der det er hensiktsmessig, omfatte tiltak for å forebygge, oppdage, reagere på, løse og kontrollere angrep som forsøker å manipulere opplæringsdatasettet (dataforgiftning), eller forhåndstrenede komponenter som brukes i opplæringen (modellforgiftning), input som er utformet for å få KI-modellen til å gjøre en feil (kontradiktoriske eksempler eller modellunndragelse), konfidensialitetsangrep eller modellfeil.

AVSNITT 3

Forpliktelser for leverandører og distributører av høyrisiko-KI-systemer og andre parter

Artikkel 16

Forpliktelser for leverandører av høyrisikosystemer for kunstig intelligens

Leverandører av høyrisikosystemer skal:

(a) sikre at deres høyrisiko-AI-systemer er i samsvar med kravene i avsnitt 2;

(b) angi på høyrisiko-AI-systemet eller, dersom dette ikke er mulig, på emballasjen eller den medfølgende dokumentasjonen, alt etter hva som er relevant, sitt navn, registrerte firmanavn eller registrerte varemerke, og adressen der de kan kontaktes;

(c) ha et kvalitetsstyringssystem på plass som er i samsvar med artikkel 17;

(d) oppbevare dokumentasjonen nevnt i artikkel 18;

(e) når de er under deres kontroll, oppbevare loggene som automatisk genereres av deres høyrisiko-AI-systemer som nevnt i artikkel 19;

(f) sikre at høyrisiko-AI-systemet gjennomgår den relevante framgangsmåten for samsvarsvurdering som nevnt i artikkel 43, før det bringes i omsetning eller tas i bruk;

(g) utarbeide en EU-samsvarserklæring i samsvar med artikkel 47;

(h) påføre CE-merkingen på høyrisiko-AI-systemet eller, dersom dette ikke er mulig, på emballasjen eller den medfølgende dokumentasjonen, for å angi samsvar med denne forordning, i samsvar med artikkel 48;

(i) oppfylle registreringsforpliktelsene nevnt i artikkel 49 nr. 1;

(j) iverksette nødvendige korrigerende tiltak og gi informasjon i henhold til artikkel 20;

(k) på begrunnet anmodning fra en nasjonal vedkommende myndighet påvise AT høyrisiko-AI-systemet ER I samsvar kravene fastsatt i avsnitt 2;

(l) sikre at høyrisiko-AI-systemet oppfyller tilgjengelighetskravene I samsvar med direktivene (EU) 2016/2102 og (EU) 2019/882.

Artikkel 17

Kvalitetsstyringssystem

1. Leverandører AV høyrisiko-AI-systemer skal innføre et kvalitetsstyringssystem som sikrer samsvar med denne forordning. Dette systemet skal dokumenteres på en systematisk og ryddig måte i form av skriftlige retningslinjer, prosedyrer og instrukser, og skal minst omfatte følgende aspekter

(a) en strategi for etterlevelse av regelverket, herunder etterlevelse av prosedyrer for samsvarsvurdering og prosedyrer for håndtering av modifikasjoner AV høyrisiko-AI-systemet;

(b) teknikker, prosedyrer og systematiske tiltak som skal brukes til design, designkontroll og designverifisering AV høyrisikosystemet;

(c) teknikker, prosedyrer og systematiske tiltak som skal brukes til utvikling, kvalitetskontroll og kvalitetssikring AV høyrisiko-AI-systemet;

(d) undersøkelses-, test- og valideringsprosedyrer som skal utføres før, under og etter utviklingen AV høyrisiko-AI-systemet, og hvor ofte de skal utføres;

(e) tekniske spesifikasjoner, herunder standarder, som skal anvendes, og, dersom de relevante harmoniserte standardene ikke anvendes fullt ut eller ikke dekker alle de relevante kravene som er fastsatt i avsnitt 2, hvilke midler som skal brukes for å sikre AT høyrisiko-AI-systemet oppfyller disse kravene;

(f) systemer og prosedyrer for datahåndtering, herunder datainnsamling, datainnsamling, dataanalyse, datamerking, datalagring, datafiltrering, datautvinning, dataaggregering, datalagring og enhver annen operasjon vedrørende dataene som utføres før og i forbindelse med markedsføring eller ibruktakelse AV høyrisiko-AI-systemer;

(g) risikostyringssystemet nevnt i artikkel 9;

(h) etablering, gjennomføring og vedlikehold av et system for overvåking etter at utstyret er brakt i omsetning, i samsvar med artikkel 72;

(i) prosedyrer knyttet til rapportering av en alvorlig hendelse i samsvar med artikkel 73;

(j) håndtering av kommunikasjon med nasjonale vedkommende myndigheter, andre relevante myndigheter, herunder de som gir eller støtter tilgang til data, meldte organer, andre operatører, kunder eller andre berørte parter;

(k) systemer og prosedyrer for registrering av all relevant dokumentasjon og informasjon;

(l) ressursforvaltning, inkludert tiltak knyttet til forsyningssikkerhet;

(m) et rammeverk for ansvarliggjøring som fastsetter ledelsens og andre ansattes ansvar med hensyn til alle aspektene som er nevnt i dette avsnittet.

2. Gjennomføringen av aspektene nevnt i nr. 1 skal stå i forhold til størrelsen på leverandørens organisasjon. Tilbyderne skal under alle omstendigheter respektere den grad av strenghet og det beskyttelsesnivå som kreves for å sikre at deres høyrisiko-AI-systemer ER i samsvar med denne forordning.

3. Tilbydere AV HØYRISIKO-AI-SYSTEMER som er underlagt forpliktelser med hensyn til kvalitetsstyringssystemer eller en tilsvarende funksjon i henhold til relevant sektorspesifikk unionsrett, kan inkludere aspektene oppført i nr. 1 som en del kvalitetsstyringssystemene i henhold til nevnte rett.

4. For tjenesteytere som er finansinstitusjoner som er underlagt krav til intern styring, ordninger eller prosesser i henhold til unionsretten om finansielle tjenester, skal plikten til å innføre et kvalitetsstyringssystem, med unntak av . 1 bokstav g), h) og i) i denne artikkel, anses for å være oppfylt ved å overholde reglene om interne styringsordninger eller prosesser i henhold til den relevante unionsretten om finansielle tjenester. For dette formål skal det tas hensyn til eventuelle harmoniserte standarder nevnt i artikkel 40.

Artikkel 18

Oppbevaring av dokumentasjon

1. Leverandøren skal I en periode på ti år etter at høyrisikosystemet er brakt i omsetning eller tatt i bruk, holde det til rådighet for de nasjonale vedkommende myndigheter:

(a) den tekniske dokumentasjonen nevnt i artikkel 11;

(b) dokumentasjonen vedrørende kvalitetsstyringssystemet nevnt i artikkel 17;

(c) dokumentasjonen vedrørende endringene som er godkjent av meldte organer, der det er aktuelt;

(d) beslutninger og andre dokumenter som er utstedt av de bemyndigede organene;

(e) EU-samsvarserklæringen nevnt i artikkel 47.

2. Hver medlemsstat skal fastsette vilkår for at dokumentasjonen nevnt i nr. 1 skal stå rådighet de nasjonale vedkommende myndigheter i den perioden som er angitt i nevnte nummer, i tilfeller der en tjenesteyter eller dennes representant som er etablert på medlemsstatens territorium, går konkurs eller opphører med sin virksomhet før utløpet av denne perioden.

3. Tilbydere som er finansinstitusjoner som er underlagt krav til intern styring, ordninger eller prosesser i henhold til Unionens lovgivning om finansielle tjenester, skal oppbevare den tekniske dokumentasjonen som en del av dokumentasjonen som oppbevares i henhold til den relevante lovgivningen om finansielle tjenester i Unionen.

Artikkel 19

Automatisk genererte logger

1. Tilbydere AV høyrisiko-ai-systemer skal oppbevare loggene nevnt i artikkel 12 nr. 1, som automatisk genereres av deres , I den utstrekning de har kontroll over slike logger. Uten at det berører gjeldende eller nasjonal rett, skal loggene oppbevares i en periode som er tilpasset det tiltenkte formålet med HØYRISIKO-AI-SYSTEMET, på minst seks måneder, med mindre annet er fastsatt i gjeldende eller nasjonal rett, særlig i unionsretten om vern av personopplysninger.

2. Tilbydere som er finansinstitusjoner som er underlagt krav til intern styring, ordninger eller prosesser i henhold til Unionens lovgivning om finansielle tjenester, skal oppbevare loggene som automatisk genereres av deres høyrisiko-AI-systemer, som en del av dokumentasjonen som oppbevares i henhold til den relevante lovgivningen om finansielle tjenester.

Artikkel 20

Korrigerende tiltak og informasjonsplikt

1. Leverandører AV høyrisiko-AI-systemer som anser eller har grunn til å anta at et høyrisiko-AI-system som de har brakt i omsetning eller tatt i bruk, ikke er i samsvar med denne forordning, skal umiddelbart treffe de nødvendige korrigerende tiltakene for å bringe systemet i samsvar med kravene i denne forordning, trekke det tilbake, sette det ut av drift eller tilbakekalle det, alt etter hva som er relevant. De skal underrette distributørene av det berørte høyrisiko-AI-systemet og, der det er relevant, installatørene, den autoriserte representanten og importørene om dette.

2. Dersom høyrisiko-AI-systemet utgjør en risiko i henhold til artikkel 79 nr. 1, og leverandøren blir på denne risikoen, skal den umiddelbart undersøke årsakene, eventuelt i samarbeid med den rapporterende driftsansvarlige, og underrette markedstilsynsmyndighetene som er kompetente for det berørte høyrisiko-AI-systemet, og eventuelt det meldte organet som utstedte et sertifikat for dette høyrisiko-AI-systemet I samsvar med artikkel 44, særlig om arten av det manglende samsvaret og om eventuelle relevante korrigerende tiltak som er truffet.

Artikkel 21

Samarbeid med kompetente myndigheter

1. Tilbydere AV høyrisiko-indikatorsystemer skal på begrunnet anmodning fra en vedkommende myndighet gi denne myndigheten all informasjon og dokumentasjon som er nødvendig for å påvise at høyrisiko-indikatorsystemet er i samsvar med kravene fastsatt i avsnitt 2, på et språk som lett kan forstås av myndigheten, på et av de offisielle språkene til Unionens institusjoner som angitt av den berørte medlemsstaten.

2. På begrunnet anmodning fra en vedkommende myndighet skal tilbydere også gi den anmodende vedkommende myndighet, alt hva som er relevant, tilgang til de automatisk genererte loggene til høyrisiko-ali-systemet nevnt i artikkel 12 nr. 1, i den grad de har kontroll over slike logger.

3. skal alle opplysninger som en vedkommende myndighet innhenter i henhold til denne artikkel, behandles i samsvar med taushetsplikten fastsatt i artikkel 78.

Artikkel 22

Autoriserte representanter for leverandører av høyrisikosystemer for kunstig intelligens

1. Før leverandører som er etablert i tredjestater, gjør sine høyrisiko-AI-systemer tilgjengelige på unionsmarkedet, skal de ved skriftlig fullmakt utpeke en autorisert representant som er etablert i Unionen.

2. Tilbyderen skal gjøre det mulig for sin autoriserte representant å utføre de oppgavene som er spesifisert i fullmakten som er mottatt fra tilbyderen.

3. Den autoriserte representanten skal utføre de oppgavene som er angitt i fullmakten fra leverandøren. Den skal på anmodning gi en kopi fullmakten til markedstilsynsmyndighetene på et av unionsinstitusjonenes offisielle språk, som angitt av vedkommende myndighet. Ved anvendelsen av denne forordning skal fullmakten gi den autoriserte representanten fullmakt til å utføre følgende oppgaver:

(a) kontrollere at EU-samsvarserklæringen nevnt i artikkel 47 og den tekniske dokumentasjonen nevnt i artikkel 11 er utarbeidet, og at leverandøren har gjennomført en egnet framgangsmåte for samsvarsvurdering;

(b) I en periode på ti år etter at høyrisiko-AI-systemet er brakt I omsetning tatt i bruk, stille kontaktopplysningene til leverandøren som utnevnte den autoriserte representanten, en kopi av EU-samsvarserklæringen nevnt I artikkel 47, den tekniske dokumentasjonen og, dersom det er relevant, sertifikatet utstedt av det meldte organet, til rådighet for vedkommende myndigheter og de nasjonale myndighetene eller organene nevnt i artikkel 74 nr. 10. b) i en periode på ti år etter at høyrisiko-AI-systemet er brakt I omsetning eller tatt i bruk

(c) på begrunnet anmodning gi en vedkommende myndighet all informasjon og dokumentasjon, herunder den som er nevnt i bokstav b) i dette ledd, som er nødvendig for å påvise at et høyrisiko-AI-system ER I samsvar med kravene fastsatt i avsnitt 2, herunder tilgang til loggene nevnt I artikkel 12 nr. 1, som automatisk genereres AV HØYRISIKO-AI-SYSTEMET, I den utstrekning slike logger er under kontroll;

(d) samarbeide med vedkommende myndigheter, på begrunnet anmodning, i forbindelse med alle tiltak som sistnevnte treffer I tilknytning til høyrisiko-ali-systemet, særlig for å redusere og avbøte risikoen som høyrisiko-ali-systemet utgjør;

(e) der det er relevant, oppfylle registreringsforpliktelsene nevnt i artikkel 49 nr. 1, eller, dersom registreringen foretas av tjenesteyteren selv, sikre at opplysningene i avsnitt A nr. 3 i vedlegg VIII ER korrekte.

Fullmakten skal gi den autoriserte representanten fullmakt til å bli kontaktet, i tillegg til eller i stedet for leverandøren, av vedkommende myndigheter i alle spørsmål knyttet til å sikre samsvar med denne forordning.

4. Den autoriserte representanten skal bringe fullmakten til opphør dersom den anser eller har grunn til å anse leverandøren opptrer i strid med sine forpliktelser i henhold til denne forordning. I så fall skal representanten umiddelbart underrette den relevante markedstilsynsmyndigheten, , dersom det er relevant, det relevante meldte organet, om oppsigelsen av fullmakten og årsakene til dette.

Artikkel 23

Importørenes forpliktelser

1. Før ET høyrisiko-AI-system bringes I omsetning, skal importøren sikre at systemet er I samsvar med denne forordning ved å kontrollere at

(a) den relevante prosedyren for samsvarsvurdering nevnt i artikkel 43 er utført av leverandøren AV høyrisiko-AI-systemet;

(b) leverandøren har utarbeidet den tekniske dokumentasjonen i samsvar med artikkel 11 og vedlegg IV;

(c) systemet er forsynt med den påkrevde CE-merkingen og er ledsaget av EU-samsvarserklæringen nevnt i artikkel 47 og bruksanvisningen;

(d) tilbyderen har utpekt en autorisert representant i samsvar med artikkel 22(1).

2. Dersom en importør har tilstrekkelig grunn til å anta at et høyrisikosystem ikke er i samsvar med denne forordning, at det er forfalsket eller ledsaget av forfalsket dokumentasjon, skal importøren ikke bringe systemet i omsetning før det er brakt I samsvar med kravene. Dersom HØYRISIKO-ANGIOGRAFISYSTEMET utgjør en risiko i henhold til artikkel 79 nr. 1, skal importøren underrette leverandøren av systemet, den autoriserte representanten og markedstilsynsmyndighetene om dette.

3. Importørene skal oppgi navn, registrert firmanavn eller registrert varemerke og adressen de kan kontaktes PÅ, I høyrisiko-AI-systemet og på emballasjen eller den medfølgende dokumentasjonen, der det er aktuelt.

4. Importørene skal, så lenge de HAR ansvar for et høyrisiko-AI-system, for at lagrings- eller transportforholdene, der det er relevant, ikke setter dets samsvar med kravene i avsnitt 2 i fare.

5. Importører skal I EN periode på ti år etter at høyrisikoalarmsystemet er brakt I omsetning eller i bruk, oppbevare en kopi av sertifikatet utstedt av det meldte organet, der det er relevant, av bruksanvisningen og av EU-samsvarserklæringen nevnt i artikkel 47.

6. Importørene skal på begrunnet anmodning gi vedkommende myndigheter alle nødvendige opplysninger og all nødvendig dokumentasjon, herunder den som ER nevnt I nr. 5, for å vise at ET høyrisiko-AI-system ER I samsvar med kravene fastsatt I avsnitt 2, på et språk som lett kan forstås av dem. For dette formål skal de også sikre at den tekniske dokumentasjonen kan gjøres tilgjengelig for disse myndighetene.

7. Importørene skal samarbeide med vedkommende myndigheter om alle tiltak disse myndighetene treffer I forbindelse med ET høyrisiko-AI-system som importørene har brakt I omsetning, særlig for å redusere og avbøte risikoene det utgjør.

Artikkel 24

Forpliktelser for distributører

1. Før distributørene gjør et høyrisiko-AI-system tilgjengelig på markedet, skal de kontrollere at det er forsynt med den påkrevde CE-merkingenat det ledsages AV en kopi av EU-samsvarserklæringen nevnt i artikkel 47 og bruksanvisningen, og at leverandøren og importøren av systemet, alt etter hva som er relevant, har oppfylt sine respektive forpliktelser som fastsatt I artikkel 16 bokstav b) og c) og artikkel 23 nr. 3.

2. Dersom en distributør på grunnlag av opplysninger han er i besittelse AV, anser eller har grunn til å anse et høyrisiko-AI-system ikke er i samsvar med kravene fastsatt i avsnitt 2, skal han ikke gjøre høyrisiko-AI-systemet tilgjengelig på markedet før systemet er brakt i samsvar med disse kravene. Dersom høyrisiko-AI-systemet utgjør en risiko i henhold til artikkel 79 nr. 1, skal distributøren dessuten underrette leverandøren eller importøren av systemet, alt etter hva som er relevant, om dette.

3. Distributørene skal, så lenge de har ansvaret for et høyrisiko-AI-system, sørge for at lagrings- eller transportforholdene, der det er relevant, ikke setter systemets samsvar med kravene i punkt 2 i fare.

4. En distributør som på grunnlag av opplysninger den er i besittelse av, anser eller har grunn til å anse at et høyrisiko-AI-system som den har gjort tilgjengelig på markedet, ikke er i samsvar med kravene fastsatt i avsnitt 2, treffe de korrigerende tiltakene som er nødvendige for å bringe systemet I samsvar med disse kravene, trekke det tilbake eller tilbakekalle det, eller skal sikre at leverandøren, importøren eller en relevant driftsansvarlig, alt etter hva som er relevant, treffer disse korrigerende tiltakene. Dersom høyrisiko-AI-systemet utgjør en risiko i henhold til artikkel 79 nr. 1, skal distributøren umiddelbart underrette leverandøren eller importøren AV systemet og vedkommende myndigheter for det berørte høyrisiko-AI-systemet, og skal særlig gi nærmere opplysninger om det manglende samsvaret og om eventuelle korrigerende tiltak som er truffet.

5. På begrunnet anmodning fra en relevant vedkommende myndighet skal distributører AV ET høyrisiko-AI-system gi denne myndigheten all informasjon og dokumentasjon om sine tiltak i henhold til nr. 1-4 som er nødvendig for å påvise at systemet er i samsvar med kravene fastsatt i avsnitt 2.

6. distributørene skal samarbeide med de relevante vedkommende myndigheter om alle tiltak disse myndighetene treffer I forbindelse med ET høyrisiko-AI-system som distributørene har gjort tilgjengelig på markedet, særlig for å redusere eller avbøte den risiko det utgjør.

Artikkel 25

Ansvar langs AI-verdikjeden

1. enhver distributør, importør, distributør eller annen tredjepart skal anses som en leverandør AV ET høyrisiko-AI-system i henhold til denne forordning og skal være underlagt leverandørens forpliktelser i henhold til artikkel 16 i alle følgende tilfeller:

(a) de setter sitt navn eller varemerke på et høyrisikosystem som allerede er markedsført eller tatt i bruk, uten at dette berører kontraktsmessige ordninger som fastsetter at forpliktelsene skal fordeles på annen måte;

(b) de foretar en vesentlig endring av et høyrisikosystem som er brakt i omsetning eller tatt i bruk på en slik måte at det forblir et høyrisikosystem i henhold til artikkel 6;

(c) de endrer det tiltenkte formålet med et aI-system, herunder et aI-system til allmenn bruk, som ikke er klassifisert som høyrisikosystem og som allerede er brakt i omsetning eller tatt i bruk, på en slik måte at det berørte AI-SYSTEMET blir et høyrisikosystem i samsvar med artikkel 6.

2. Dersom omstendighetene nevnt i nr. 1 inntreffer, skal den leverandøren som opprinnelig brakte aI-systemet i omsetning eller tok det i bruk, ikke lenger anses for å være en leverandør av det spesifikke aI-systemet i henhold til denne forordning. Den opprinnelige leverandøren skal samarbeide nært med nye leverandører og skal stille til rådighet de nødvendige opplysningene og gi den tekniske tilgangen og annen bistand som med rimelighet kan forventes, og som er nødvendig for å oppfylle forpliktelsene fastsatt i denne forordning, særlig med hensyn til samsvarsvurderingen AV høyrisiko-AI-systemer. Dette ledd får ikke anvendelse i tilfeller der den opprinnelige leverandøren klart har spesifisert at vedkommendes AI-SYSTEM ikke skal endres til et høyrisiko-ai-system, og derfor ikke omfattes av plikten til å utlevere dokumentasjonen.

3. Når det gjelder høyrisiko-AI-systemer som er sikkerhetskomponenter i produkter som omfattes av Unionens harmoniseringslovgivning oppført i avsnitt A I vedlegg I, skal produktprodusenten anses for å være leverandøren AV HØYRISIKO-AI-SYSTEMET, og skal være underlagt forpliktelsene i henhold til artikkel 16 under en av følgende omstendigheter

(a) høyrisiko-AI-systemet markedsføres sammen med produktet under produktprodusentens navn eller varemerke;

(b) høyrisiko-AI-systemet tas i bruk under produktprodusentens navn eller varemerke etter at produktet er kommet på markedet.

4. Leverandøren AV et høyrisiko-ai-system og tredjeparten som leverer et , verktøy, tjenester, komponenter eller prosesser som brukes eller integreres i et høyrisiko-ai-system, skal ved skriftlig avtale spesifisere nødvendig informasjon, kapasitet, teknisk tilgang og annen bistand basert på det allment anerkjente tekniske nivået, for å gjøre det mulig for leverandøren av høyrisiko-ai-systemet å oppfylle forpliktelsene fastsatt i denne forordning fullt ut. Dette ledd ikke anvendelse på tredjeparter som gjør verktøy, tjenester, prosesser eller komponenter, fra generelle aI-modeller, tilgjengelige for allmennheten under en lisens med fri og åpen kildekode.

aI-kontoret kan utvikle og anbefale frivillige standardvilkår for kontrakter mellom leverandører av og tredjeparter som leverer verktøy, tjenester, komponenter eller prosesser som brukes til eller er integrert i høyrisiko-ai-systemer. Ved utarbeidelsen av disse frivillige standardvilkårene skal aI-kontoret ta hensyn til mulige kontraktskrav som gjelder i bestemte sektorer eller forretningssaker. De frivillige standardvilkårene skal offentliggjøres og være gratis tilgjengelige i et lett anvendelig elektronisk format.

5. Nr. 2 og 3 berører ikke behovet for å overholde og beskytte immaterielle rettigheter, fortrolig forretningsinformasjon og forretningshemmeligheter i samsvar med unionsretten og nasjonal rett.

Artikkel 26

Forpliktelser for brukere av høyrisikosystemer med kunstig intelligens

1. de som utplasserer høyrisikosystemer FOR KUNSTIG INTELLIGENS, skal treffe egnede tekniske og organisatoriske tiltak for å sikre at de bruker slike systemer i samsvar med bruksanvisningen som følger med systemene, i henhold til nr. 3 og 6.

2. Utplasseringsselskapene skal overlate det menneskelige tilsynet til fysiske personer som har nødvendig kompetanse, opplæring og myndighet, samt nødvendig støtte.

3. Forpliktelsene fastsatt i nr. 1 og 2 berører ikke andre forpliktelser for utplasseringsselskapet i henhold til unionsretten eller nasjonal rett og utplasseringsselskapets frihet til å organisere sine egne ressurser og aktiviteter med henblikk på å gjennomføre de tiltakene for menneskelig tilsyn som leverandøren har angitt.

4. Uten at det berører nr. 1 og 2, skal den driftsansvarlige, i den grad den driftsansvarlige utøver kontroll over inndataene, sikre at inndataene er relevante og tilstrekkelig representative med tanke på det tiltenkte formålet med høyrisiko-AI-systemet.

5. utplasserere skal overvåke driften AV HØYRISIKO-AI-SYSTEMET på grunnlag av bruksanvisningen og, dersom det er relevant, underrette leverandørene I samsvar med artikkel 72. Dersom utplasserere har grunn til å anta at bruken av høyrisiko-AI-systemet I samsvar med bruksanvisningen kan føre til at dette aI-systemet utgjør en risiko i henhold til artikkel 79 nr. 1, skal de uten unødig opphold underrette leverandøren eller distributøren og den relevante markedstilsynsmyndigheten, og skal stanse bruken av systemet. Dersom utplasserere har identifisert en alvorlig hendelse, skal de også umiddelbart underrette først leverandøren, og deretter importøren eller distributøren og de relevante markedstilsynsmyndighetene om hendelsen. Dersom utrulleren ikke er i stand til å nå leverandøren, skal artikkel 73 få *tilsvarende* anvendelse. Denne forpliktelsen skal ikke omfatte sensitive driftsopplysninger hos utplasserere AV KI-systemer som er rettshåndhevende myndigheter.

For distributører som er finansinstitusjoner som er underlagt krav til sin interne styring, sine ordninger eller prosesser i henhold til Unionens lovgivning om finansielle tjenester, skal overvåkingsplikten fastsatt i første ledd anses å være oppfylt ved å overholde reglene om interne styringsordninger, prosesser og mekanismer i henhold til den relevante lovgivningen om finansielle tjenester.

6. De som utplasserer høyrisiko-AI-systemer, skal oppbevare loggene som automatisk genereres av det aktuelle høyrisiko-AI-systemet, i den grad de har kontroll over slike logger, i en periode som er tilpasset det tiltenkte formålet med , på minst seks måneder, med mindre annet er fastsatt i gjeldende unionsrett eller nasjonal rett, særlig unionsretten om vern av personopplysninger.

Distributører som er finansinstitusjoner som er underlagt krav til intern styring, ordninger eller prosesser i henhold til Unionens lovgivning om finansielle tjenester, skal føre loggene som en del av dokumentasjonen som oppbevares i henhold til den relevante lovgivningen om finansielle tjenester i Unionen.

7. Før et høyrisiko-AI-system tas i bruk eller brukes på arbeidsplassen, skal utplasserere som er arbeidsgivere, informere arbeidstakernes representanter og de berørte arbeidstakerne om at de vil være gjenstand for bruk AV HØYRISIKO-AI-SYSTEMET. Denne informasjonen skal, der det er relevant, gis i samsvar med reglene og framgangsmåtene fastsatt i unionsretten og nasjonal rett og praksis om informasjon til arbeidstakerne og deres representanter.

8. utplasserere av HØYRISIKO-AI-SYSTEMER som er offentlige myndigheter eller unionsinstitusjoner, -organer, -kontorer eller -byråer, skal overholde registreringsforpliktelsene nevnt i artikkel 49. Dersom slike ibruktakere oppdager AT høyrisiko-AI-systemet de planlegger å bruke, ikke er registrert i EU-databasen nevnt i artikkel 71, skal de ikke bruke dette systemet og skal underrette leverandøren eller distributøren om dette.

9. Der det er relevant, skal de som tar i bruk høyrisiko-AI-systemer, bruke informasjonen som gis i henhold til artikkel 13 i denne forordning, til å oppfylle sin plikt til å gjennomføre en vurdering av personvernkonsekvenser i henhold til artikkel 35 i forordning (EU) 2016/679 eller artikkel 27 i direktiv (EU) 2016/680.

10. Uten at det berører direktiv (EU) 2016/680, skal den som tar i bruk et høyrisiko AI-system for biometrisk identifikasjon i etterkant av en etterforskning med sikte på målrettet ransaking AV en person SOM ER mistenkt eller dømt for å ha begått en straffbar handling, anmode om tillatelse på *forhånd* eller uten ugrunnet opphold og senest innen 48 timer fra en rettslig myndighet eller en forvaltningsmyndighet hvis beslutning er bindende og kan prøves rettslig, eller uten unødig opphold og senest innen 48 timer, av en rettslig myndighet eller en forvaltningsmyndighet hvis avgjørelse er bindende og kan prøves rettslig, for bruk systemet, unntatt når det brukes til innledende identifisering av en potensiell mistenkt på grunnlag av objektive og verifiserbare fakta som er direkte knyttet til lovbruddet. Hver bruk skal begrenses til det som er strengt nødvendig for etterforskningen av en bestemt straffbar handling.

Dersom tillatelsen som det er anmodet om i henhold til første ledd, avslås, skal bruken av det biometriske identifikasjonssystemet etter fjernkontroll som er knyttet til den anmodede tillatelsen, stanses med umiddelbar virkning, og personopplysningene knyttet til bruken AV høyrisikoidentifikasjonssystemet som det ble anmodet om tillatelse til, skal slettes.

Et slikt høyrisikosystem for biometrisk identifikasjon etter skal under ingen omstendigheter brukes til rettshåndhevelsesformål på en ikke-målrettet måte, uten noen forbindelse til en straffbar handling, en straffesak, en reell og aktuell eller reell og forutsigbar trussel om en straffbar handling eller søket etter en bestemt savnet person. Det skal sikres at rettshåndhevelsesmyndighetene ikke kan treffe noen beslutning som har negative rettsvirkninger for en person, utelukkende på grunnlag av resultatene fra slike systemer for biometrisk identifikasjon etter fjernavlesning.

Dette avsnittet berører ikke artikkel 9 i forordning (EU) 2016/679 og artikkel 10 i direktiv (EU) 2016/680 om behandling av biometriske opplysninger.

Uavhengig av formål eller bruker skal enhver bruk av slike høyrisiko-AI-systemer dokumenteres i DEN relevante og skal gjøres tilgjengelig for den relevante markedstilsynsmyndigheten og den nasjonale personvernmyndigheten på anmodning, med unntak av utlevering av sensitive driftsopplysninger knyttet til rettshåndhevelse. Dette ledd skal ikke berøre tilsynsmyndighetenes myndighet i henhold til direktiv (EU) 2016/680.

skal utplasseringsselskapene sende inn årlige rapporter til de relevante markedstilsynsmyndighetene og nasjonale datatilsynsmyndighetene om sin bruk av biometriske identifikasjonssystemer etter utplassering, med unntak av utlevering av sensitive driftsopplysninger knyttet til rettshåndhevelse. Rapportene kan aggregeres for å dekke mer enn én utplassering.

Medlemsstatene kan, i samsvar med unionsretten, innføre mer restriktive lover om bruk av biometriske identifikasjonssystemer etter fjernavlesning.

11. Uten at det berører artikkel 50 i denne forordning, skal utplasserere AV HØYRISIKO-AI-SYSTEMER nevnt i vedlegg III som treffer beslutninger eller bistår med å treffe beslutninger knyttet til fysiske personer, informere de fysiske personene om at de er underlagt bruken av HØYRISIKO-AI-SYSTEMET. For HØYRISIKO-AI-SYSTEMER som brukes til rettshåndhevingsformål, får artikkel 13 i direktiv (EU) 2016/680 anvendelse.

12. utplasseringsselskapene skal samarbeide med de relevante vedkommende myndigheter i alle tiltak som disse myndighetene treffer i forbindelse med høyrisiko-AI-systemet for å gjennomføre denne forordning.

Artikkel 27

Konsekvensanalyse av AI-systemer med høy risiko for grunnleggende rettigheter

1. Før utplassering av et høyrisiko-AI-system nevnt i artikkel 6 nr. 2, med unntak av høyrisiko-AI-systemer som skal brukes på området oppført i nr. 2 I vedlegg III, utplasserere som er offentligrettslige organer eller private enheter som yter offentlige tjenester, og utplasserere av høyrisiko-AI-systemer nevnt i . 5 bokstav b) og c) i vedlegg III, foreta en vurdering av innvirkningen på de grunnleggende rettighetene som bruken av et slikt system kan få. For dette formål skal de som tar i bruk systemet, foreta en vurdering som består av

(a) en beskrivelse av utbyggerens prosesser der høyrisiko-AI-systemet vil bli brukt i tråd med det tiltenkte formålet;

(b) en beskrivelse av tidsrommet og hyppigheten som hvert høyrisikosystem ER ment å bli brukt innenfor;

(c) hvilke kategorier av fysiske personer og grupper som kan bli berørt av bruken i den spesifikke konteksten;

(d) de spesifikke risikoene for skade som sannsynligvis vil ha innvirkning på de kategoriene av fysiske personer eller grupper av personer som er identifisert i henhold til bokstav c) i dette ledd, idet det tas hensyn til opplysningene som leverandøren har gitt i henhold til artikkel 13;

(e) en beskrivelse av gjennomføringen av tiltak for tilsyn med mennesker, i henhold til bruksanvisningen;

(f) hvilke tiltak som skal iverksettes dersom disse risikoene materialiserer seg, herunder ordninger for intern styring og klagemekanismer.

2. Forpliktelsen fastsatt i nr. 1 gjelder ved første gangs bruk AV høyrisiko-AI-systemet. I lignende tilfeller kan den som tar i bruk systemet, basere seg på tidligere gjennomførte konsekvensutredninger av grunnleggende rettigheter eller eksisterende konsekvensutredninger utført av leverandøren. Dersom utrulleren under bruken av HØYRISIKO-INFORMASJONSINNHENTINGSSYSTEMET anser at noen av elementene som er oppført i nr. 1, har endret seg eller ikke lenger er oppdatert, skal utrulleren treffe de nødvendige tiltak for å oppdatere informasjonen.

3. Når vurderingen nevnt i nr. 1 i denne artikkel er utført, skal driftsansvarlige underrette markedstilsynsmyndigheten om resultatene og sende inn den utfylte malen nevnt i nr. 5 i denne artikkel som en del av underretningen. I tilfellet nevnt i artikkel 46 nr. 1 kan driftsansvarlige unntas fra denne .

4. Dersom noen av forpliktelsene fastsatt i denne artikkel allerede er oppfylt gjennom konsekvensanalysen av personvern som er gjennomført i henhold til artikkel 35 i forordning (EU) 2016/679 eller artikkel 27 i direktiv (EU) 2016/680, skal konsekvensanalysen av grunnleggende rettigheter nevnt i nr. 1 i denne artikkel utfylle den konsekvensanalysen av personvern.

5. AI-kontoret skal utvikle en mal for et spørreskjema, blant annet gjennom et automatisert verktøy, for å gjøre det enklere for utplassører å oppfylle sine forpliktelser i henhold til denne artikkelen på en forenklet måte.

AVSNITT 4

Meldende myndigheter og meldte organer

Artikkel 28

Varsling til myndighetene

1. Hver medlemsstat skal utpeke eller opprette minst én meldermyndighet med ansvar for å utarbeide og gjennomføre de nødvendige framgangsmåtene for vurdering, utpeking og melding av samsvarsvurderingsorganer og for overvåking av disse. Disse framgangsmåtene skal utarbeides i samarbeid mellom de meldende myndighetene i alle medlemsstatene.

2. Medlemsstatene kan beslutte at vurderingen og overvåkingen nevnt i nr. 1 skal utføres av et nasjonalt akkrediteringsorgan i henhold til og i samsvar med forordning (EF) nr. 765/2008.

3. Meldende myndigheter skal opprettes, organiseres og drives på en slik måte at det ikke oppstår interessekonflikter med samsvarsvurderingsorganer, og at objektiviteten og upartiskheten i deres virksomhet ivaretas.

4. Meldende myndigheter skal være organisert på en slik måte at beslutninger om melding av samsvarsvurderingsorganer treffes av andre kompetente personer enn dem som utførte vurderingen av disse organene.

5. Meldende myndigheter skal verken tilby eller yte aktiviteter som samsvarsvurderingsorganer utfører, konsulenttjenester på kommersiell eller konkurransemessig basis.

6. Meldende myndigheter skal sikre konfidensialiteten til informasjonen de innhenter, i samsvar med artikkel 78.

7. Meldingsmyndighetene skal ha et tilstrekkelig antall kompetente medarbeidere til rådighet for å kunne utføre sine oppgaver på en tilfredsstillende måte. Det kompetente personellet skal ha den nødvendige ekspertisen, der det er relevant, for sin funksjon, på områder som informasjonsteknologi, AI og jus, herunder tilsyn med grunnleggende rettigheter.

Artikkel 29

Søknad fra et samsvarsvurderingsorgan om notifikasjon

1. Samsvarsvurderingsorganer skal sende inn en søknad om notifikasjon til notifiserende myndighet i den medlemsstaten der de er etablert.

2. Søknaden om melding skal ledsages av en beskrivelse av samsvarsvurderingsvirksomheten, samsvarsvurderingsmodulen eller -modulene og de typer KI-systemer som samsvarsvurderingsorganet hevder å ha kompetanse , samt av et eventuelt akkrediteringsbevis utstedt av et nasjonalt akkrediteringsorgan, som bekrefter at samsvarsvurderingsorganet oppfyller kravene fastsatt i artikkel 31.

ethvert gyldig dokument knyttet til eksisterende utpekinger av det søkende meldte organet i henhold til annen EU-harmoniseringslovgivning skal legges til.

3. Dersom det berørte samsvarsvurderingsorganet ikke kan framlegge et akkrediteringssertifikat, skal det framlegge for meldermyndigheten all dokumentasjon som er nødvendig for verifisering, anerkjennelse og regelmessig overvåking av at det oppfyller kravene fastsatt i artikkel 31.

4. For meldte organer som er utpekt i henhold til annen EU-harmoniseringslovgivning, kan alle dokumenter og sertifikater knyttet til disse utpekingene brukes til å underbygge deres utpekingsprosedyre i henhold til denne forordning, alt etter hva som er hensiktsmessig. Det meldte organet skal oppdatere dokumentasjonen nevnt i nr. 2 og 3 i denne artikkel når det skjer relevante endringer, slik at myndigheten med ansvar for meldte organer kan overvåke og kontrollere at alle kravene fastsatt i artikkel 31 til enhver tid er oppfylt.

Artikkel 30

Prosedyre for varsling

1. Meldende myndigheter kan bare melde samsvarsvurderingsorganer som har oppfylt kravene fastsatt i artikkel 31.

2. Meldingsmyndighetene skal ved hjelp av det elektroniske meldingsverktøyet som er utviklet og forvaltes av Kommisjonen, underrette Kommisjonen og de andre om hvert samsvarsvurderingsorgan nevnt i nr. 1.

3. Meldingen nevnt i nr. 2 i denne artikkel skal inneholde fullstendige opplysninger om samsvarsvurderingsvirksomheten, samsvarsvurderingsmodulen eller -modulene, de berørte typene AV AI-systemer og den relevante kompetanseattesten. Dersom en melding ikke er basert på et akkrediteringssertifikat som nevnt i artikkel 29 nr. 2, skal meldermyndigheten framlegge for Kommisjonen og de andre medlemsstatene dokumentasjon som bekrefter samsvarsvurderingsorganets kompetanse og de ordninger som er innført for å sikre at dette organet vil bli overvåket regelmessig og fortsatt vil oppfylle kravene fastsatt i artikkel 31.

4. Det berørte samsvarsvurderingsorganet kan utøve virksomheten til et meldt organ bare dersom Kommisjonen eller de andre medlemsstatene ikke har reist innvendinger innen to uker etter en melding fra en meldermyndighet dersom den omfatter et akkrediteringssertifikat som nevnt i artikkel 29 nr. 2, eller innen to måneder etter en melding fra meldermyndigheten dersom den omfatter dokumentasjon som nevnt i artikkel 29 nr. 3.

5. Dersom det reises innvendinger, skal Kommisjonen uten opphold innlede samråd med de berørte medlemsstatene og samsvarsvurderingsorganet. På bakgrunn av dette skal Kommisjonen avgjøre om godkjenningen er berettiget. Kommisjonen skal rette sin beslutning til den berørte medlemsstaten og til det relevante samsvarsvurderingsorganet.

Artikkel 31

Krav til meldte organer

1. ET meldt organ skal være opprettet i henhold til nasjonal lovgivning i en medlemsstat og skal være en juridisk person.

2. Meldte organer skal oppfylle kravene til organisasjon, kvalitetsstyring, ressurser og prosesser som er nødvendige for å utføre sine oppgaver, samt egnede krav til cybersikkerhet.

3. De meldte organenes organisasjonsstruktur, ansvarsfordeling, rapporteringslinjer og drift skal sikre tillit til deres arbeid og til resultatene av samsvarsvurderingsaktivitetene som de utfører.

4. Meldte organer skal være uavhengige av leverandøren av et HØYRISIKO-AI-SYSTEM som de utfører samsvarsvurderingsaktiviteter I forbindelse med. Meldte organer skal også være uavhengige av enhver annen aktør som har en økonomisk interesse i vurderte HØYRISIKO-AI-SYSTEMER, samt av leverandørens eventuelle konkurrenter. Dette skal ikke være til hinder for bruk av vurderte HØYRISIKO-AI-SYSTEMER som er nødvendige for samsvarsvurderingsorganets virksomhet, eller for bruk av slike HØYRISIKO-AI-SYSTEMER til personlige formål.

5. Verken et samsvarsvurderingsorgan, dets øverste ledelse eller personalet som er ansvarlig for å utføre samsvarsvurderingsoppgavene, skal være direkte involvert i konstruksjon, utvikling, markedsføring eller bruk AV høyrisiko-AI-systemer, og de skal heller ikke representere partene som ER involvert i disse aktivitetene. De skal ikke delta i noen aktivitet som kan komme i konflikt deres uavhengighet eller integritet i forbindelse med samsvarsvurderingsaktiviteter som de er meldt for. Dette skal særlig gjelde konsulenttjenester.

6. Meldte organer skal organiseres og drives på en slik måte at de sikrer uavhengighet, objektivitet og upartiskhet i sin virksomhet. Meldte organer skal dokumentere og iverksette en struktur og prosedyrer for sikre upartiskhet og for å fremme og anvende prinsippene om upartiskhet i hele sin organisasjon, sitt personale og sine vurderingsaktiviteter.

7. Meldte organer skal ha dokumenterte framgangsmåter som sikrer at deres personale, komiteer, datterforetak, underleverandører og eventuelle tilknyttede organer eller personale i eksterne organer i samsvar med artikkel 78 behandler opplysninger som de kommer i besittelse av under utførelsen av samsvarsvurderingsaktiviteter, konfidensielt, unntatt når det er lovpålagt å offentliggjøre dem. Personalet ved meldte organer skal ha taushetsplikt med hensyn til alle opplysninger de får kjennskap til under utførelsen av sine oppgaver i henhold til denne forordning, unntatt overfor meldermyndighetene i den medlemsstat der de utøver sin virksomhet.

8. Meldte organer skal ha prosedyrer for utførelse av aktiviteter som behørig hensyn til leverandørens størrelse, sektoren den opererer i, dens struktur og graden av kompleksitet I det aktuelle AI-systemet.

9. Meldte organer skal tegne en passende ansvarsforsikring for sin samsvarsvurderingsvirksomhet, med mindre ansvaret overtas av medlemsstaten der de er etablert i samsvar med nasjonal lovgivning, eller denne medlemsstaten selv er direkte ansvarlig for samsvarsvurderingen.

10. Meldte organer skal være i stand til å utføre alle sine oppgaver i henhold til denne forordning med den høyeste grad av faglig integritet og den nødvendige kompetanse på det spesifikke området, enten disse oppgavene utføres av meldte organer selv eller på deres vegne og under deres ansvar.

11. Meldte organer skal ha tilstrekkelig intern kompetanse til effektivt å kunne evaluere oppgavene som utføres eksterne parter på deres vegne. Det meldte organet skal ha permanent tilgang til tilstrekkelig administrativt, teknisk, juridisk og vitenskapelig personell som har erfaring med OG kunnskap om de relevante typene KI-systemer, data og databehandling, og som oppfyller kravene fastsatt i avsnitt 2.

12. Meldte organer skal delta i samordningsaktiviteter som nevnt i artikkel 38. De skal også delta direkte eller være representert i europeiske standardiseringsorganisasjoner, eller sikre at de er kjent med og oppdatert med hensyn til relevante standarder.

Artikkel 32

Formodning om samsvar med kravene til meldte organer

Dersom et samsvarsvurderingsorgan viser at det er i samsvar med kriteriene fastsatt i de relevante harmoniserte standardene eller deler av disse, hvis henvisninger er offentliggjort i *Den europeiske unions tidende*, skal det anses å være samsvar med kravene i artikkel 31 i den grad de gjeldende harmoniserte standardene dekker disse kravene.

Artikkel 33

Datterselskaper av meldte organer og underleveranser

1. Dersom et meldt organ gir bestemte oppgaver i forbindelse med samsvarsvurderingen i oppdrag til underleverandører eller benytter seg av et datterforetak, skal det sikre at underleverandøren eller datterforetaket oppfyller kravene fastsatt i artikkel 31, og skal underrette meldermyndigheten om dette.

2. Meldte organer skal ta fullt ansvar for de oppgavene som utføres av eventuelle underleverandører eller datterselskaper.

3. aktiviteter kan bare settes ut til underleverandører eller utføres av et datterselskap etter samtykke fra leverandøren. Meldte organer skal offentliggjøre en liste over sine datterselskaper.

4. De relevante dokumentene vedrørende vurderingen av underleverandørens eller datterforetakets kvalifikasjoner og det arbeidet som er utført av dem i henhold til denne forordning, skal holdes til rådighet for den anmeldende myndighet i en periode på fem år fra datoen for underleveransens opphør.

Artikkel 34

Operasjonelle forpliktelser for meldte organer

1. Meldte organer skal verifisere samsvar for høyrisiko-AI-systemer I samsvar med framgangsmåtene for samsvarsvurdering fastsatt i artikkel 43.

2. Meldte organer skal unngå unødvendige byrder for leverandørene når de utøver sin virksomhet, og ta behørig hensyn til leverandørens størrelse, sektoren den driver virksomhet i, dens struktur og graden av kompleksitet I det berørte høYRISIKO-AI-SYSTEMET, særlig med sikte å minimere de administrative byrdene og samsvarskostnadene for mikroforetak og små foretak i henhold til rekommandasjon 2003/361/EF. Det meldte organet skal likevel respektere den grad av strenghet og det beskyttelsesnivået som kreves for at høyrisiko-AI-systemet skal være I samsvar kravene i denne forordning.

3. Meldte organer skal gjøre all relevant dokumentasjon, herunder leverandørens dokumentasjon, tilgjengelig for meldermyndigheten nevnt i artikkel 28 og på anmodning oversende den til denne for å gjøre det mulig for meldermyndigheten å gjennomføre sin vurdering, utpeking, melding og overvåking, og for å lette vurderingen som er beskrevet i dette avsnitt.

Artikkel 35

Identifikasjonsnumre og lister over meldte organer

1. Kommisjonen skal tildele ett enkelt identifikasjonsnummer til hvert organ som er meldt, selv om organet er meldt i henhold til mer enn én unionsrettsakt.

2. Kommisjonen skal offentliggjøre en liste over organer som er meldt i henhold til denne forordning, herunder deres identifikasjonsnummer og de aktiviteter de er meldt for. Kommisjonen skal sikre at listen holdes oppdatert.

Artikkel 36

Endringer i varsler

1. Meldingsmyndigheten skal underrette Kommisjonen og de andre medlemsstatene om alle relevante endringer i meldingen av et meldt organ ved hjelp av det elektroniske meldingsverktøyet nevnt i artikkel 30 nr. 2.

2. Fremgangsmåtene fastsatt i artikkel 29 og 30 skal gjelde for utvidelser av meldingens virkeområde.

For andre endringer i meldingen enn utvidelser av dens virkeområde skal prosedyrene fastsatt i nr. 3 til 9 få anvendelse.

3. Dersom et meldt organ beslutter å opphøre med sin samsvarsvurderingsvirksomhet, skal det underrette meldermyndigheten og de berørte leverandørene om dette så snart som mulig og, dersom det er planlagt å opphøre, minst ett år før virksomheten opphører. Sertifikatene til det meldte organet kan fortsatt være gyldige i ni måneder etter at det meldte organets virksomhet er opphørt, forutsatt at et annet meldt organ skriftlig har bekreftet at det vil påta seg ansvaret for høyrisikosystemene som omfattes av disse sertifikatene. Det sistnevnte meldte organet skal fullføre en fullstendig vurdering av de berørte HØYRISIKO-AI-SYSTEMENE innen utløpet av denne ni måneders perioden før det utsteder nye sertifikater for disse systemene. Dersom det meldte organet har opphørt sin virksomhet, skal meldermyndigheten trekke tilbake utpekingen.

4. Dersom en meldermyndighet har tilstrekkelig grunn til å at et meldt organ ikke lenger oppfyller kravene fastsatt i artikkel 31, eller at det ikke oppfyller sine forpliktelser, skal meldermyndigheten uten opphold undersøke saken med den største omhu. I den forbindelse skal den underrette det berørte meldte organet om de innvendingene som er reist, og gi det mulighet til å gi for sitt syn. Dersom meldermyndigheten konkluderer med at det meldte organet ikke lenger oppfyller kravene fastsatt i artikkel 31, eller at det ikke oppfyller sine forpliktelser, skal den begrense, midlertidig eller tilbakekalle utpekingen, avhengig av hvor alvorlig den manglende oppfyllelsen av disse kravene eller oppfyllelsen av disse forpliktelsene er. Den skal umiddelbart underrette Kommisjonen og de øvrige medlemsstatene om dette.

5. Dersom utpekingen er suspendert, begrenset eller helt delvis trukket tilbake, skal det meldte organet informere de berørte leverandørene om dette innen ti dager.

6. Dersom en utpeking begrenses, midlertidig oppheves eller trekkes tilbake, skal meldermyndigheten treffe egnede tiltak for å sikre at det berørte meldte organets arkiver oppbevares, og for å gjøre dem tilgjengelige for meldermyndigheter i andre medlemsstater og for markedstilsynsmyndigheter på deres anmodning.

7. Ved begrensning, midlertidig opphevelse eller tilbaketrekking av en utpeking skal den anmeldende myndighet

(a) vurdere virkningen på sertifikatene som er utstedt av det meldte organet;

(b) legge fram en rapport om sine funn for Kommisjonen og de andre medlemsstatene innen tre måneder etter at endringene i utpekingen er meddelt;

(c) kreve at det meldte organet, innen en rimelig frist fastsatt av myndigheten, suspenderer eller tilbakekaller eventuelle sertifikater som er utstedt urettmessig, for å sikre at høyrisikosystemer på markedet fortsatt er I samsvar med kravene;

(d) informere Kommisjonen og medlemsstatene om sertifikater som den har krevd suspendert eller trukket tilbake;

(e) gi de nasjonale vedkommende myndigheter i den medlemsstat der tjenesteyteren har sitt registrerte forretningssted, all relevant informasjon om sertifikatene som den har krevd suspendert eller trukket tilbake; denne myndigheten skal om nødvendig treffe egnede tiltak for å unngå en potensiell risiko for helse, sikkerhet eller grunnleggende rettigheter.

8. Med unntak av sertifikater som er urettmessig utstedt, og der en betegnelse er suspendert eller begrenset, skal sertifikatene fortsatt være gyldige under en av følgende omstendigheter

(a) meldermyndigheten har bekreftet, innen en måned etter suspensjonen eller begrensningen, at det ikke er noen risiko for helse, sikkerhet eller grunnleggende rettigheter i forbindelse med sertifikater som berøres av suspensjonen eller begrensningen, og meldermyndigheten har skissert en tidsplan for tiltak for å avhjelpe suspensjonen eller begrensningen; eller

(b) meldermyndigheten har bekreftet at ingen sertifikater som er relevante for opphevelsen, vil bli utstedt, endret eller utstedt på nytt i løpet av perioden for opphevelsen eller begrensningen, og oppgir om det meldte organet har kapasitet til å fortsette å overvåke og fortsatt være ansvarlig for eksisterende sertifikater som er utstedt i løpet av perioden for opphevelsen eller begrensningen; Dersom meldermyndigheten fastslår at det meldte organet ikke har kapasitet til å støtte eksisterende utstedte sertifikater, skal leverandøren av systemet som omfattes av sertifikatet, innen tre måneder etter opphevelsen eller begrensningen skriftlig bekrefte overfor vedkommende nasjonale myndigheter i den medlemsstaten vedkommende har sitt registrerte forretningssted, at et annet kvalifisert meldt organ midlertidig overtar det meldte organets funksjoner for å overvåke og fortsatt være ansvarlig for sertifikatene den perioden opphevelsen eller begrensningen varer.

9. Med unntak av sertifikater som er utstedt urettmessig, og der en utpeking er trukket tilbake, skal sertifikatene være gyldige i en periode på ni måneder under følgende omstendigheter

(a) den nasjonale vedkommende myndighet I medlemsstaten der leverandøren av høyrisiko-ali-systemet som omfattes av sertifikatet har sitt registrerte forretningssted, har bekreftet at det ikke er noen risiko for helse, sikkerhet eller grunnleggende rettigheter forbundet med de aktuelle HØYRISIKO-ALI-SYSTEMENE, og

(b) et annet meldt organ har skriftlig bekreftet at det vil påta seg det umiddelbare ansvaret for disse AI-systemene og fullføre sin vurdering innen 12 måneder etter at utpekingen er trukket tilbake.

Under de omstendigheter som er nevnt i første ledd, kan vedkommende nasjonale myndighet i den medlemsstat der leverandøren av systemet som omfattes av sertifikatet, har sitt forretningssted, forlenge sertifikatenes midlertidige gyldighet med ytterligere perioder på tre måneder, som til sammen ikke skal overstige tolv måneder.

Den nasjonale vedkommende myndighet eller det meldte organet som overtar funksjonene til det meldte organet som berøres av endringen av utpekingen, skal umiddelbart underrette Kommisjonen, de øvrige medlemsstatene og de andre meldte organene om dette.

Artikkel 37

Utfordring av kompetansen til meldte organer

1. Kommisjonen skal om nødvendig undersøke alle tilfeller der det er til å tvile på et meldt organs kompetanse eller på at et meldt organ fortsatt oppfyller kravene fastsatt i artikkel 31 og sitt gjeldende ansvar.

2. Meldingsmyndigheten skal på anmodning gi Kommisjonen alle relevante opplysninger om meldingen eller opprettholdelsen av det berørte meldte organets kompetanse.

3. Kommisjonen skal sikre at all sensitiv informasjon som innhentes i løpet av dens undersøkelser i henhold til denne artikkel, behandles konfidensielt i samsvar med artikkel 78.

4. Dersom Kommisjonen konstaterer at et meldt organ ikke oppfyller eller ikke lenger oppfyller kravene for sin utpeking, skal den underrette den medlemsstat som har utpekt organet, om dette og anmode den om å treffe de nødvendige korrigerende tiltak, herunder om nødvendig midlertidig oppheve eller tilbakekalle utpekingen. Dersom medlemsstaten ikke treffer de nødvendige korrigerende tiltakene, kan Kommisjonen ved hjelp av en gjennomføringsrettsakt midlertidig oppheve, begrense eller trekke tilbake utpekingen. Denne gjennomføringsrettsakten skal vedtas i samsvar med undersøkelsesprosedyren nevnt i artikkel 98 nr. 2.

Artikkel 38

Koordinering av meldte organer

1. Kommisjonen skal sikre at det med hensyn til høyrisikosystemer FOR KUNSTIG INTELLIGENS etableres og drives hensiktsmessig samordning og samarbeid mellom meldte organer som er aktive i framgangsmåtene for samsvarsvurdering i henhold til denne forordning, i form av en sektorgruppe av meldte organer.

2. Hver notifiserende myndighet skal sikre at de organene den har notifisert, deltar i arbeidet i en gruppe nevnt i nr. 1, direkte eller gjennom utpekte representanter.

3. Kommisjonen skal sørge for utveksling av kunnskap og beste praksis mellom notifiserende myndigheter.

Artikkel 39

Samsvarsvurderingsorganer i tredjeland

Samsvarsvurderingsorganer som er opprettet i henhold til lovgivningen i en tredjestat som Unionen har inngått en avtale med, kan gis tillatelse til å den virksomhet som utøves av meldte organer i henhold til denne forordning, forutsatt at de oppfyller kravene fastsatt i artikkel 31 eller sikrer et tilsvarende samsvarsnivå.

AVSNITT 5

Standarder, samsvarsvurdering, sertifikater, registrering

Artikkel 40

Harmoniserte standarder og standardiseringsleveranser

1. Høyrisiko-AI-systemer eller allsidige AI-modeller som er i samsvar med harmoniserte standarder eller deler av disse, hvis henvisninger er offentliggjort i *Den europeiske unions tidende* i samsvar med forordning (EU) nr. 1025/2012, skal anses å være i samsvar med kravene fastsatt i avsnitt 2 i dette kapittel eller, alt etter hva som er relevant, med forpliktelsene fastsatt i kapittel V avsnitt 2 og 3 i denne forordning, i utstrekning disse standardene dekker disse kravene eller forpliktelsene.

2. I samsvar med artikkel 10 forordning (EU) nr. 1025/2012 skal Kommisjonen uten unødig utstede standardiseringsanmodninger som omfatter alle kravene fastsatt i avsnitt 2 i dette kapittel, og, dersom det er relevant, standardiseringsanmodninger som omfatter forpliktelsene fastsatt i kapittel V avsnitt 2 og 3 i denne forordning. Standardiseringsanmodningen skal også be om leveranser om rapporterings- og dokumentasjonsprosesser for å forbedre KI-systemers ressursytelse, f.eks. ved å redusere høyrisiko KI-systemers forbruk av energi og andre ressurser løpet av deres livssyklus, og om energieffektiv utvikling av generelle KI-modeller. Når Kommisjonen utarbeider en anmodning om standardisering, skal den rådføre seg med styret og relevante interessenter, herunder det rådgivende forumet.

Når Kommisjonen utsteder en standardiseringsanmodning til europeiske standardiseringsorganisasjoner, skal den spesifisere at standardene skal være klare og konsistente, herunder med standardene som er utarbeidet i de ulike sektorene for produkter som omfattes den eksisterende unionsharmoniseringslovgivningen oppført I vedlegg I, og ha som mål sikre at høyrisikosystemer eller allsidige AI-modeller som bringes i omsetning eller tas i bruk i Unionen, oppfyller de relevante kravene eller forpliktelsene som er fastsatt i denne forordning.

Kommisjonen skal anmode de europeiske standardiseringsorganisasjonene om å dokumentere at de har gjort sitt beste for å oppfylle målene nevnt i første og annet ledd i dette nummer i samsvar med artikkel 24 i forordning (EU) nr. 1025/2012.

3. Deltakerne i standardiseringsprosessen skal søke å fremme investeringer og nyskaping PÅ OMRÅDET for KUNSTIG intelligens, blant annet ved å øke rettssikkerheten, samt konkurranseevnen og veksten i unionsmarkedet, bidra til å styrke det globale samarbeidet om standardisering og ta hensyn til eksisterende internasjonale standarder PÅ OMRÅDET FOR KUNSTIG INTELLIGENS SOM ER forenlige med Unionens verdier, grunnleggende rettigheter og interesser, og styrke flerpartsforvaltning som sikrer balansert representasjon av interesser og effektiv deltakelse av alle relevante interessenter I samsvar med artikkel 5, 6 og 7 i forordning (EU) nr. 1025/2012.

Artikkel 41

Felles spesifikasjoner

1. Kommisjonen kan vedta gjennomføringsrettsakter som fastsetter felles spesifikasjoner for kravene i avsnitt 2 i dette kapittel eller, alt etter hva som er relevant, for forpliktelsene fastsatt i avsnitt 2 og 3 i kapittel V, dersom følgende vilkår er oppfylt

(a) Kommisjonen i henhold til artikkel 10 nr. 1 i forordning (EU) nr. 1025/2012 har anmodet en eller flere europeiske standardiseringsorganisasjoner om å utarbeide en harmonisert standard for kravene i avsnitt 2 i dette kapittel, eller, alt etter hva som er relevant, for forpliktelsene fastsatt i avsnitt 2 og 3 i kapittel V, og:

   (i) forespørselen ikke er akseptert av noen av de europeiske standardiseringsorganisasjonene; eller

(ii) de harmoniserte standardene som omhandler denne anmodningen, ikke leveres innen den fristen som er fastsatt i samsvar med artikkel 10 nr. 1 i forordning (EU) nr. 1025/2012, eller

(iii) de relevante harmoniserte standardene ikke i tilstrekkelig grad ivaretar hensynet til grunnleggende rettigheter; eller

(iv) de harmoniserte standardene ikke er i samsvar med anmodningen; og

(b) ingen henvisning til harmoniserte standarder som dekker kravene nevnt i avsnitt 2 i dette kapittel eller, der det er relevant, forpliktelsene nevnt i avsnitt 2 og 3 i kapittel V, er offentliggjort i *Den europeiske unions* tidende samsvar med forordning (EU) nr. 1025/2012, og det forventes ikke at en slik henvisning vil bli innen rimelig tid.

Ved utarbeidelsen av de felles spesifikasjonene skal Kommisjonen rådføre seg med det rådgivende forumet nevnt i artikkel 67.

Gjennomføringsrettsaktene nevnt i første ledd i dette nummer skal vedtas i samsvar med framgangsmåten for behandling nevnt i artikkel 98 nr. 2.

2. Før Kommisjonen utarbeider et utkast til gjennomføringsrettsakt, skal den underrette komiteen nevnt i artikkel 22 i forordning (EU) nr. 1025/2012 om at den anser vilkårene fastsatt i nr. 1 i denne artikkel for å være oppfylt.

3. Høyrisiko-AI-systemer eller generelle AI-modeller som er i samsvar med de felles spesifikasjonene nevnt i nr. 1, eller deler av disse spesifikasjonene, skal anses å være i samsvar med kravene fastsatt i avsnitt 2 i dette kapittel eller, alt etter som er relevant, å være i samsvar med forpliktelsene nevnt i avsnitt 2 og 3 i kapittel V, i den utstrekning de felles spesifikasjonene dekker disse kravene eller disse forpliktelsene.

4. Dersom en harmonisert standard er vedtatt av en europeisk standardiseringsorganisasjon og foreslått for Kommisjonen med sikte på *offentliggjøring* av en henvisning til *den i Den europeiske unions* tidende, skal Kommisjonen vurdere den harmoniserte standarden i samsvar med forordning (EU) nr. 1025/2012. Når henvisningen til en harmonisert standard *offentliggjøres* i *Den europeiske unions* tidende, skal Kommisjonen oppheve gjennomføringsrettsaktene nevnt nr. 1 deler av disse som omfatter de samme kravene fastsatt i avsnitt 2 i dette kapittel eller, alt etter hva som er relevant, de samme forpliktelsene fastsatt i avsnitt 2 og 3 i kapittel V.

5. Dersom leverandører av høyrisiko-AI-systemer eller generelle aI-modeller ikke overholder de felles spesifikasjonene nevnt i nr. 1, skal de behørig begrunne at de har vedtatt tekniske løsninger som oppfyller kravene nevnt i avsnitt 2 i dette kapittel eller, alt etter hva som er relevant, oppfyller forpliktelsene fastsatt i avsnitt 2 og 3 i kapittel V på et nivå som minst tilsvarer disse.

6. Dersom en medlemsstat mener at en felles spesifikasjon ikke fullt ut oppfyller kravene i avsnitt 2 eller, alt etter hva som er relevant, ikke oppfyller forpliktelsene i kapittel V avsnitt 2 og 3, skal den underrette Kommisjonen om dette og gi en detaljert forklaring. Kommisjonen skal vurdere disse opplysningene og, dersom det er hensiktsmessig, endre gjennomføringsrettsakten om fastsettelse av den berørte felles spesifikasjonen.

Artikkel 42

Formodning om samsvar med visse krav

1. Høyrisiko-AI-systemer som er opplært og testet på data som gjenspeiler de spesifikke geografiske, atferdsmessige, kontekstuelle eller funksjonelle omgivelsene de er ment å brukes i, skal antas å være i samsvar med de relevante kravene fastsatt i artikkel 10 nr. 4.

2. Høyrisiko-AI-systemer som er sertifisert, eller for hvilke det er utstedt en samsvarserklæring i henhold til en cybersikkerhetsordning I samsvar med forordning (EU) 2019/881, og hvis henvisninger er offentliggjort i *Den europeiske unions* tidende, skal anses å oppfylle cybersikkerhetskravene fastsatt I artikkel 15 i denne forordning i den grad cybersikkerhetssertifikatet eller samsvarserklæringen eller deler av disse dekker disse kravene.

Artikkel 43

Vurdering av samsvar

1. For høyrisiko-AI-systemer oppført i nr. 1 i vedlegg III, der leverandøren, for å påvise at et høyrisiko-AI-system er I samsvar med kravene fastsatt i avsnitt 2, har anvendt harmoniserte standarder som nevnt i artikkel 40, eller, der det er relevant, felles spesifikasjoner som nevnt i artikkel 41, skal leverandøren velge en av følgende framgangsmåter for samsvarsvurdering basert på

(a) den interne kontrollen nevnt i vedlegg VI; eller

(b) vurderingen av kvalitetsstyringssystemet og vurderingen av den tekniske dokumentasjonen, med medvirkning av et meldt organ, som nevnt i vedlegg VII.

Ved påvisning av at et høyrisiko-AI-system er i samsvar med kravene fastsatt i avsnitt 2, skal leverandøren følge framgangsmåten for samsvarsvurdering fastsatt i vedlegg VII der:

(a) harmoniserte standarder som nevnt i artikkel 40 ikke finnes, og felles spesifikasjoner som nevnt i artikkel 41 ikke er tilgjengelige;

(b) leverandøren ikke har brukt, eller bare har brukt deler av, den harmoniserte standarden;

(c) de felles spesifikasjonene nevnt i bokstav a) finnes, men leverandøren har ikke tatt dem i bruk;

(d) en eller flere av de harmoniserte standardene nevnt i bokstav a) er publisert med en begrensning, og bare på den delen av standarden som ble begrenset.

Med henblikk på framgangsmåten for samsvarsvurdering nevnt i vedlegg VII kan leverandøren velge hvilket som helst av de meldte organene. Dersom høyrisiko-AI-systemet er beregnet på å bli tatt i bruk av rettshåndhevelses-, innvandrings- eller asylmyndigheter eller av Unionens institusjoner, organer, kontorer eller byråer, skal imidlertid markedstilsynsmyndigheten nevnt i artikkel 74 nr. 8 eller 9, alt etter hva som er relevant, fungere som meldt organ.

2. For høyrisikosystemer som nevnt I nr. 2 til 8 i vedlegg III, skal leverandørene følge framgangsmåten for samsvarsvurdering basert på internkontroll som nevnt i vedlegg VI, som ikke foreskriver at et meldt organ skal involveres.

3. For høyrisiko-AI-systemer som omfattes av Unionens harmoniseringslovgivning oppført i avsnitt A i vedlegg I, skal leverandøren følge relevante framgangsmåten for samsvarsvurdering som kreves i henhold til disse rettsaktene. Kravene fastsatt avsnitt 2 i dette kapittel skal få anvendelse på disse høyrisiko-AI-systemene og skal være en del av denne vurderingen. Punkt 4.3, 4.4, .5 og punkt 4.6 femte ledd i vedlegg VII skal også få anvendelse.

Med henblikk på denne vurderingen skal meldte organer som er meldt i henhold til disse rettsaktene, ha rett til å kontrollere AT høyrisiko-AI-systemene er I samsvar med kravene fastsatt I avsnitt 2, forutsatt at disse meldte organenes samsvar med kravene fastsatt i artikkel 31 . 4, 5, 10 og 11 er blitt vurdert I forbindelse meldingsprosedyren i henhold til disse rettsaktene.

Dersom en rettsakt oppført i avsnitt A i vedlegg I gjør det mulig for produktprodusenten å velge bort en tredjeparts samsvarsvurdering, forutsatt at produsenten har anvendt alle harmoniserte standarder som dekker alle de relevante kravene, kan produsenten bare benytte seg av denne muligheten dersom den også har anvendt harmoniserte standarder eller, dersom det er relevant, felles spesifikasjoner nevnt i artikkel 41, som dekker alle kravene fastsatt i avsnitt 2 i dette kapittel.

4. Høyrisikosystemer som allerede har vært gjenstand for en samsvarsvurderingsprosedyre, skal gjennomgå en ny samsvarsvurderingsprosedyre I tilfelle en vesentlig endring, uavhengig av om det endrede systemet skal distribueres videre eller fortsatt brukes av den nåværende distributøren.

For høyrisiko-AI-systemer som fortsetter å lære etter at de er brakt i omsetning eller tatt i bruk, skal endringer av høyrisiko-AI-systemet og dets ytelse som er forhåndsbestemt av leverandøren på tidspunktet for den første samsvarsvurderingen, og som er en del av informasjonen i den tekniske dokumentasjonen nevnt i nr. 2 bokstav f) i vedlegg IV, ikke utgjøre en vesentlig endring.

5. Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 for å endre vedlegg VI og VII ved å oppdatere dem i lys av den tekniske utviklingen.

6. Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 for å endre nr. 1 og 2 i denne artikkel med henblikk på å underlegge høyrisikosystemer som nevnt i nr. 2-8 I vedlegg III, framgangsmåten for samsvarsvurdering nevnt i vedlegg VII eller deler av den. Kommisjonen skal vedta slike delegerte rettsakter idet den tar hensyn til hvor effektiv framgangsmåten for samsvarsvurdering basert på internkontroll nevnt i vedlegg VI er når det gjelder å forebygge eller minimere den risiko for helse og sikkerhet og vern av grunnleggende rettigheter som slike systemer utgjør, samt til tilgjengeligheten av tilstrekkelig kapasitet og ressurser blant meldte organer.

Artikkel 44

Sertifikater

1. Sertifikater utstedt av meldte organer i samsvar med vedlegg VII skal være avfattet på et språk som lett kan forstås av de relevante myndighetene i den medlemsstat der det meldte organet er etablert.

2. Sertifikater skal være gyldige i den perioden de angir, som ikke skal overstige fem år for AI-systemer som omfattes AV vedlegg I, og fire år for AI-systemer som omfattes av vedlegg III. på anmodning fra leverandøren kan gyldigheten av et sertifikat forlenges med ytterligere perioder, som hver ikke skal overstige fem år for AI-SYSTEMER som omfattes av vedlegg I, og fire år for AI-SYSTEMER som omfattes av vedlegg III, på grunnlag av en ny samsvarsvurdering i samsvar med gjeldende prosedyrer for samsvarsvurdering. ethvert tillegg til et sertifikat skal forbli gyldig, forutsatt at sertifikatet som det supplerer, er .

3. Dersom et meldt organ finner at ET KI-system ikke lenger oppfyller kravene fastsatt i avsnitt 2, skal det, idet det tas hensyn til forholdsmessighetsprinsippet, midlertidig oppheve eller trekke tilbake det utstedte sertifikatet eller pålegge det restriksjoner, med mindre systemleverandøren gjennom egnede korrigerende tiltak innen en passende frist fastsatt av det meldte organet sikrer at disse kravene oppfylles. Det meldte organet skal begrunne sin beslutning.

det skal en framgangsmåte for å klage på beslutninger truffet av de meldte organene, herunder på utstedte samsvarssertifikater.

Artikkel 45

Meldte organers informasjonsforpliktelser

1. Meldte organer skal informere meldermyndigheten om følgende:

(a) eventuelle unionssertifikater for vurdering av teknisk dokumentasjon, eventuelle tillegg til disse sertifikatene og eventuelle godkjenninger av kvalitetsstyringssystemer utstedt i samsvar med kravene i vedlegg VII;

(b) ethvert avslag, enhver begrensning, suspensjon eller tilbaketrekking av et unionssertifikat for vurdering av teknisk dokumentasjon eller en godkjenning av et kvalitetsstyringssystem utstedt i samsvar med kravene i vedlegg VII;

(c) eventuelle omstendigheter som påvirker omfanget av eller vilkårene for varsling;

(d) enhver anmodning om informasjon som de har mottatt fra markedstilsynsmyndigheter om samsvarsvurderingsaktiviteter;

(e) på forespørsel, samsvarsvurderingsaktiviteter som utføres innenfor rammen av deres melding, og enhver annen aktivitet som utføres, herunder grenseoverskridende aktiviteter og underleveranser.

2. Hvert meldt organ skal informere de andre meldte organene om dette:

(a) godkjenninger av kvalitetsstyringssystemer som den har avslått, suspendert eller trukket tilbake, og, på anmodning, om godkjenninger av kvalitetsstyringssystemer som den har utstedt;

(b) Unionens sertifikater for vurdering av teknisk dokumentasjon eller eventuelle tillegg til disse som den har avslått, trukket tilbake, suspendert eller på annen måte begrenset, og, på anmodning, de sertifikater og/eller tillegg til disse som den har utstedt.

3. Hvert meldt organ skal gi de andre meldte organene som utfører tilsvarende samsvarsvurderingsaktiviteter for de samme typene AI-systemer, relevant informasjon om spørsmål knyttet til negative og, på anmodning, positive resultater av samsvarsvurderinger.

4. Meldte organer skal sikre konfidensialiteten til informasjonen de innhenter, i samsvar med artikkel 78.

Artikkel 46

Unntak fra prosedyren for samsvarsvurdering

1. Som unntak fra artikkel 43 og etter en behørig begrunnet anmodning kan enhver markedstilsynsmyndighet gi tillatelse til AT bestemte høyrisikosystemer bringes i omsetning eller tas i bruk på den berørte medlemsstatens territorium, av særlige grunner knyttet til offentlig sikkerhet eller vern av menneskers liv og helse, miljøvern eller vern av viktige industri- og infrastrukturanlegg. Denne tillatelsen skal være tidsbegrenset mens de nødvendige framgangsmåtene for samsvarsvurdering gjennomføres, idet det tas hensyn til de særlige grunnene som begrunner unntaket. Disse framgangsmåtene skal fullføres uten unødig forsinkelse.

2. I en behørig begrunnet hastesituasjon av særlige hensyn til den offentlige sikkerhet eller i tilfelle av en spesifikk, vesentlig og overhengende trussel mot fysiske personers liv eller fysiske sikkerhet kan rettshåndhevelsesmyndigheter eller sivilbeskyttelsesmyndigheter ta et spesifikt høyrisiko-AI-system I bruk uten tillatelsen nevnt i nr. 1, forutsatt at det anmodes om en slik tillatelse under eller etter bruken uten unødig forsinkelse. Dersom tillatelsen nevnt i nr. 1 nektes, skal bruken AV HØYRISIKO-AI-SYSTEMET stanses med umiddelbar virkning, og alle resultater og utdata fra slik bruk skal umiddelbart kasseres.

3. Tillatelsen nevnt i . 1 skal utstedes bare dersom markedstilsynsmyndigheten konkluderer med AT høyrisiko-AI-systemet oppfyller kravene i avsnitt 2. Markedstilsynsmyndigheten skal underrette Kommisjonen og de andre medlemsstatene om enhver tillatelse som er utstedt i henhold til nr. 1 og 2. Denne plikten skal ikke omfatte sensitive driftsopplysninger i forbindelse med rettshåndhevende myndigheters virksomhet.

4. Dersom verken en medlemsstat eller Kommisjonen innen 15 kalenderdager etter mottak av opplysningene nevnt i nr. 3 har reist innvendinger en tillatelse utstedt av en markedstilsynsmyndighet i en medlemsstat i samsvar med nr. 1, skal denne tillatelsen anses som berettiget.

5. Dersom en medlemsstat innen 15 kalenderdager etter mottak av meldingen nevnt i nr. 3 gjør innvendinger mot en tillatelse utstedt av en markedstilsynsmyndighet en annen medlemsstat, eller dersom Kommisjonen anser tillatelsen for å være i strid med unionsretten, eller dersom medlemsstatenes konklusjon med hensyn til systemets samsvar som nevnt i nr. 3, er ubegrunnet, skal Kommisjonen uten opphold innlede samråd med den berørte medlemsstaten. De berørte driftsansvarlige skal konsulteres og ha mulighet til å legge fram sine synspunkter. På bakgrunn av dette skal Kommisjonen avgjøre om tillatelsen er berettiget. Kommisjonen skal rette sin beslutning til den berørte medlemsstaten og til de berørte driftsansvarlige.

6. Dersom Kommisjonen anser tillatelsen som uberettiget, skal den trekkes tilbake av markedstilsynsmyndigheten i den berørte medlemsstaten.

7. For høyrisikosystemer knyttet til produkter som omfattes av Unionens harmoniseringslovgivning oppført i avsnitt A i vedlegg I, skal bare unntakene fra samsvarsvurderingen som er fastsatt i denne Unionens harmoniseringslovgivning, få anvendelse.

Artikkel 47

EU-samsvarserklæring

1. Tilbyderen skal utarbeide en skriftlig, maskinlesbar, fysisk eller elektronisk signert EU-samsvarserklæring for hvert høyrisiko-AI-system, og holde den tilgjengelig for nasjonale vedkommende myndigheter I ti år etter at høyrisiko-AI-systemet er brakt I omsetning eller tatt i bruk. EU-samsvarserklæringen skal identifisere høyrisiko-AI-systemet som den er for. EN kopi av EU-samsvarserklæringen skal på anmodning framlegges for de relevante nasjonale vedkommende myndigheter.

2. I EU-samsvarserklæringen skal det angis at det berørte høyrisiko-AI-systemet oppfyller kravene fastsatt avsnitt 2. EU-samsvarserklæringen skal inneholde opplysningene fastsatt i vedlegg V og skal oversettes til et språk som lett kan forstås av vedkommende nasjonale myndigheter I de medlemsstatene der HØYRISIKO-AI-SYSTEMET bringes i omsetning eller gjøres tilgjengelig.

3. Dersom høyrisiko-AI-systemer er underlagt annen EU-harmoniseringslovgivning som også krever en EU-samsvarserklæring, skal det utarbeides én enkelt EU-samsvarserklæring for all unionslovgivning som får anvendelse på høyrisiko-AI-systemet. Erklæringen skal inneholde alle opplysninger som er nødvendige for å identifisere den harmoniseringslovgivningen i Unionen som erklæringen gjelder.

4. Ved å utarbeide EU-samsvarserklæringen påtar leverandøren seg ansvaret for at kravene i punkt 2 oppfylles. Tilbyderen skal holde EU-samsvarserklæringen oppdatert etter behov.

5. Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 for å endre vedlegg V ved å oppdatere innholdet i EU-samsvarserklæringen som er fastsatt i vedlegget, for å innføre elementer som blir nødvendige i lys av den tekniske utviklingen.

Artikkel 48

CE-merking

1. CE-merkingen skal være underlagt de generelle prinsippene som er fastsatt i artikkel 30 i forordning (EF) nr. 765/2008.

2. For høyrisikosystemer som leveres digitalt, skal digital CE-merking bare brukes hvis den er lett tilgjengelig via grensesnittet som systemet er tilgjengelig fra, eller via en lett tilgjengelig maskinlesbar kode eller andre elektroniske midler.

3. CE-merkingen skal påføres synlig, lett leselig og uutslettelig FOR . Dersom dette ikke er mulig eller ikke er berettiget på grunn av HØYRISIKO-AI-SYSTEMETS art, skal det påføres emballasjen eller den medfølgende dokumentasjonen, alt etter hva som er hensiktsmessig.

4. Dersom det er relevant, skal CE-merkingen etterfølges av identifikasjonsnummeret til det meldte organet som er ansvarlig framgangsmåtene for samsvarsvurdering fastsatt i artikkel 43. meldte organets identifikasjonsnummer skal påføres av organet selv eller, etter dets anvisninger, av leverandøren eller av leverandørens representant. Identifikasjonsnummeret skal også angis i alt reklamemateriell som nevner at høyrisiko-AI-systemet oppfyller kravene til CE-merking.

5. Dersom høyrisiko-AI-systemer er underlagt annen unionslovgivning som også foreskriver CE-merking, skal CE-merkingen angi at høyrisiko-AI-systemet også oppfyller kravene i denne andre lovgivningen.

Artikkel 49

Registrering

1. Før et høyrisiko-AI-system oppført i vedlegg III bringes i omsetning eller tas i bruk, med unntak av HØYRISIKO-AI-SYSTEMER nevnt i nr. 2 i vedlegg III, skal leverandøren eller, dersom det er relevant, den autoriserte representanten registrere seg selv og sitt system i EU-databasen nevnt i artikkel 71.

2. Før et AI-system som leverandøren har konkludert med at det ikke utgjør en høy risiko i henhold til artikkel 6 nr. 3, bringes I omsetning eller tas i bruk, skal leverandøren eller, dersom det er relevant, den autoriserte representanten registrere seg selv og systemet i EU-databasen nevnt i artikkel 71.

3. Før ibruktaking eller bruk av et høyrisiko-AI-system oppført i vedlegg III, med unntak av høyrisiko-AI-systemer oppført i nr. 2 I vedlegg III, skal utplasserere som er offentlige myndigheter, unionsinstitusjoner, -organer, -kontorer eller -byråer eller personer som opptrer på deres vegne, registrere seg selv, velge systemet og registrere bruken av det I EU-databasen nevnt I artikkel 71.

4. For høyrisiko-AI-systemer nevnt i nr. 1, 6 og 7 i vedlegg III, på områdene rettshåndhevelse, migrasjon, asyl og grensekontrollforvaltning, skal registreringen nevnt nr. 1, 2 og 3 i denne artikkel skje I en sikker, ikke-offentlig del av EU-databasen nevnt i artikkel 71 og skal bare inneholde følgende opplysninger, alt etter hva som er relevant, nevnt i

(a) Avsnitt A, punkt 1 til 10, i vedlegg VIII, med unntak av punkt 6, 8 og 9;

(b) Del B, punkt 1 til 5, og punkt 8 og 9 i vedlegg VIII;

(c) Del C, punkt 1 til 3, i vedlegg VIII;

(d) punktene 1, 2, 3 og 5 i vedlegg IX.

Bare Kommisjonen og de nasjonale myndighetene nevnt i artikkel 74 nr. 8 skal ha tilgang til de respektive begrensede delene av EU-databasen som er oppført i første ledd i dette nummer.

5. Høyrisiko-AI-systemer som nevnt i nr. 2 i vedlegg III skal registreres på nasjonalt nivå.

CHaPTER IV

KRAV TIL ÅPENHET FOR LEVERANDØRER OG DISTRIBUTØRER AV VISSE AI-SYSTEMER

Artikkel 50

Transparensforpliktelser for leverandører og distributører av visse AI-systemer

1. Tilbydere skal sikre at KI-systemer som er beregnet på å samhandle direkte med fysiske personer, er utformet og utviklet på en slik måte at de berørte fysiske personene blir informert om at de samhandler med et KI-system, med mindre dette er åpenbart for en fysisk person som er rimelig velinformert, oppmerksom og veloverveid, omstendighetene og brukssammenhengen tatt i betraktning. Denne forpliktelsen får ikke anvendelse på AI-SYSTEMER som ved lov er godkjent for å avdekke, forebygge, etterforske eller straffeforfølge straffbare handlinger, med forbehold om passende garantier for tredjeparters rettigheter og friheter, med mindre disse systemene er tilgjengelige for allmennheten for å anmelde en straffbar handling.

2. Tilbydere av AI-systemer, herunder generelle AI-SYSTEMER, som genererer syntetisk lyd-, bilde-, video- eller tekstinnhold, skal sikre at utdataene fra AI-systemet er merket i et maskinlesbart format og kan oppdages som kunstig generert eller manipulert. Tilbyderne skal sikre at deres tekniske løsninger er effektive, samvirkende, robuste og pålitelige så langt det er teknisk mulig, idet det tas hensyn til særtrekkene ved og begrensningene for ulike typer innhold, kostnadene ved gjennomføringen og det allment anerkjente tekniske nivået, slik dette kan gjenspeiles i relevante tekniske standarder. Denne forpliktelsen gjelder ikke i DEN utstrekning KI-systemene utfører en hjelpefunksjon for standardredigering eller ikke i vesentlig grad endrer inngangsdataene som leveres av eller semantikken i disse, eller i tilfeller der dette er tillatt ved lov for å oppdage, forebygge, etterforske eller straffeforfølge straffbare handlinger.

3. De som tar i bruk et system for emosjonsgjenkjenning eller et biometrisk kategoriseringssystem, skal informere de fysiske personene som er eksponert for dette, om hvordan systemet fungerer, og skal behandle personopplysningene i samsvar med forordning (EU) 2016/679 og (EU) 2018/1725 og direktiv (EU) 2016/680, alt etter hva som er relevant. Denne forpliktelsen skal ikke gjelde for AI-systemer som brukes til biometrisk kategorisering og følelsesgjenkjenning, som er tillatt ved lov for å oppdage, forebygge eller etterforske straffbare handlinger, med forbehold om passende garantier for tredjeparters rettigheter og friheter, og i samsvar med unionsretten.

4. brukere av et KI-system som genererer eller manipulerer bilde-, lyd- eller videoinnhold som utgjør en dyp forfalskning, skal opplyse om at innholdet er kunstig generert eller manipulert. Denne plikten gjelder ikke dersom bruken er hjemlet i lov for å avdekke, forebygge, etterforske eller straffeforfølge straffbare handlinger. Dersom innholdet inngår i et åpenbart kunstnerisk, kreativt, satirisk, fiktivt eller lignende verk eller program, er forpliktelsene til åpenhet i dette ledd begrenset til å opplyse om eksistensen av slikt generert eller manipulert innhold på en hensiktsmessig måte som ikke hindrer visningen eller nytelsen av verket.

den som bruker et KI-system som genererer eller manipulerer tekst som publiseres med det formål informere allmennheten om forhold av offentlig interesse, skal opplyse om at teksten er kunstig generert eller manipulert. Denne plikten gjelder ikke når bruken er hjemlet i lov for å avdekke, forebygge, etterforske eller straffeforfølge straffbare handlinger, eller når det KI-GENERERTE innholdet har gjennomgått en prosess med menneskelig gjennomgang eller redaksjonell kontroll og en fysisk eller juridisk person har det redaksjonelle ansvaret for publiseringen av innholdet.

5. Opplysningene nevnt i nr. 1-4 skal gis til de berørte fysiske personene på en klar og tydelig måte senest på tidspunktet for den første interaksjonen eller eksponeringen. Informasjonen skal være i samsvar med gjeldende krav til tilgjengelighet.

6. Nr. 1-4 skal ikke berøre kravene og forpliktelsene fastsatt i kapittel III, og skal ikke berøre andre åpenhetsforpliktelser fastsatt i unionsretten eller nasjonal rett for utplasserere AV AI-systemer.

7. AI-kontoret skal oppmuntre til og legge til rette for at det utarbeides regler for god praksis på unionsplan for å lette en effektiv gjennomføring av forpliktelsene med hensyn til påvisning og merking av kunstig generert eller manipulert innhold. Kommisjonen kan vedta gjennomføringsrettsakter for å godkjenne disse retningslinjene for god praksis i samsvar med framgangsmåten fastsatt i artikkel 56 nr. 6. Dersom Kommisjonen anser at retningslinjene ikke er tilstrekkelige, kan den vedta en gjennomføringsrettsakt som fastsetter felles regler for gjennomføringen av disse forpliktelsene i samsvar med framgangsmåten for undersøkelse fastsatt i artikkel 98 nr. 2.

CHaPTER V

GENERELLE AI-MODELLER

AVSNITT 1

Klassifiseringsregler

Artikkel 51

Klassifisering av generelle KI-modeller som generelle KI-modeller med systemrisiko

1. EN generell KI-modell skal klassifiseres som en GENERELL KI-modell med systemrisiko dersom den oppfyller ett eller flere av følgende vilkår:

(a) den har stor gjennomslagskraft, evaluert på grunnlag av egnede tekniske verktøy og metoder, inkludert indikatorer og referanseverdier;

(b) på grunnlag av en beslutning truffet av Kommisjonen, på *eget initiativ* eller etter en kvalifisert varsling fra det vitenskapelige panelet, har evner eller virkninger som tilsvarer dem som er angitt i bokstav a), idet det tas hensyn til kriteriene fastsatt i vedlegg XIII.

2. EN generell AI-modell skal antas å ha høy påvirkningsevne i henhold til nr. 1 bokstav a) når den kumulative beregningsmengden som brukes til opplæring av den, målt i flyttalloperasjoner, er større enn 10^{25}.

3. Kommisjonen skal vedta delegerte rettsakter i samsvar med artikkel 97 for å endre terskelverdiene oppført i nr. 1 og 2 i denne artikkel, samt for å supplere referanseverdier og indikatorer i lys av den teknologiske utviklingen, f.eks. algoritmiske forbedringer eller økt maskinvareeffektivitet, når det er nødvendig, for at disse terskelverdiene skal gjenspeile det aktuelle tekniske nivået.

Artikkel 52

Fremgangsmåte

1. Dersom en generell AI-modell oppfyller vilkåret nevnt i artikkel 51 nr. 1 bokstav a), skal den relevante leverandøren underrette Kommisjonen om dette uten opphold og under alle omstendigheter innen to uker etter at kravet er oppfylt eller det blir kjent at det vil bli oppfylt. Meldingen skal inneholde de opplysninger som er nødvendige for å påvise at det relevante kravet er oppfylt. Dersom Kommisjonen blir oppmerksom på en generell aI-modell som innebærer systemrisiko, og som den ikke har fått melding om, kan den beslutte å utpeke den som en modell med systemrisiko.

2. Tilbyderen av en generell aI-modell som oppfyller vilkåret nevnt i artikkel 51 nr. 1 bokstav a), kan sammen med meldingen legge fram tilstrekkelig underbygde argumenter for å påvise at den generelle aI-modellen unntaksvis, selv om den oppfyller dette kravet, på grunn av sine særlige egenskaper ikke utgjør noen systemrisiko og derfor ikke bør klassifiseres som en generell AI-MODELL med systemrisiko.

3. Dersom Kommisjonen konkluderer med at argumentene som er fremsatt i henhold til nr. 2, ikke er tilstrekkelig underbygget, og den relevante tilbyder ikke har kunnet påvise at den generelle aI-modellen på grunn av sine særlige egenskaper ikke medfører systemrisiko, skal Kommisjonen avvise disse argumentene, og den generelle aI-modellen skal anses for å være en generell aI-modell med systemrisiko.

4. Kommisjonen kan på eget *initiativ* eller etter et kvalifisert varsel fra det vitenskapelige panelet I henhold til artikkel 90 nr. 1 a) utpeke en generell KI-modell som systemrisiko, på grunnlag av kriteriene fastsatt i vedlegg XIII.

Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 for å endre vedlegg XIII ved å spesifisere og oppdatere kriteriene som er fastsatt i nevnte vedlegg.

5. På begrunnet anmodning fra en tilbyder hvis modell er blitt utpekt som en generell aI-modell med systemrisiko i henhold til nr. 4, skal Kommisjonen ta hensyn til anmodningen og kan beslutte å revurdere om DEN GENERELLE aI-modellen fortsatt kan anses å utgjøre en systemrisiko på grunnlag av kriteriene fastsatt i vedlegg XIII. En slik anmodning skal inneholde objektive, detaljerte og nye grunner som har oppstått siden utpekingsbeslutningen. Tilbydere kan anmode om ny vurdering tidligst seks måneder etter utpekingsbeslutningen. Dersom Kommisjonen etter sin revurdering beslutter å opprettholde utpekingen som en generell aI-modell med systemrisiko, kan tilbydere anmode om revurdering tidligst seks måneder etter denne beslutningen.

6. Kommisjonen skal sikre at det offentliggjøres en liste over generelle KI-modeller med systemrisiko, og skal holde denne listen oppdatert, uten at det berører behovet for å overholde og beskytte immaterielle rettigheter og fortrolig forretningsinformasjon eller forretningshemmeligheter i samsvar med unionsretten og nasjonal rett.

AVSNITT 2

Forpliktelser for leverandører av generelle AI-modeller

Artikkel 53

Forpliktelser for leverandører av generelle AI-modeller

1. Leverandører av generelle AI-modeller skal:

(a) utarbeide og ajourføre den tekniske dokumentasjonen for modellen, herunder opplæringen og testprosessen og resultatene av evalueringen, som minst skal inneholde informasjonen angitt I vedlegg XI, slik at den på anmodning kan utleveres til AI-kontoret og de nasjonale vedkommende myndigheter;

(b) , holde oppdatert og gjøre tilgjengelig informasjon og dokumentasjon for leverandører av KI-systemer som har hensikt å integrere den generelle KI-modellen i sine KI-systemer. Uten at det berører behovet for å overholde og beskytte immaterielle rettigheter og fortrolige forretningsopplysninger eller forretningshemmeligheter i samsvar med unionsretten og nasjonal rett, skal informasjonen og dokumentasjonen

(i) gjøre det mulig for leverandører av aI-systemer å ha en god forståelse av mulighetene og begrensningene ved den generelle aI-modellen og å overholde sine forpliktelser i henhold til denne forordning, og

(ii) minst inneholde de elementene som er angitt i vedlegg XII;

(c) innføre retningslinjer for å overholde unionsretten om opphavsrett og beslektede rettigheter, og særlig for å identifisere og overholde, blant annet ved hjelp av toppmoderne teknologi, et forbehold om rettigheter som er uttrykt i henhold til artikkel 4(3) i direktiv (EU) 2019/790;

(d) utarbeide og offentliggjøre et tilstrekkelig detaljert sammendrag om innholdet som brukes til opplæring i den generelle aI-modellen, i henhold til en mal fra aI-kontoret.

2. Forpliktelsene fastsatt i . 1 bokstav a) og b) får ikke anvendelse på leverandører AV aI-modeller som er utgitt under en lisens med fri og åpen kildekode som tillater tilgang, bruk, endring og distribusjon av modellen, og hvis parametere, herunder vektene, informasjonen om modellarkitekturen og informasjonen om modellbruk, er gjort offentlig tilgjengelig. Dette unntaket skal ikke gjelde for generelle aI-modeller med systemrisiko.

3. Tilbydere av generelle aI-modeller skal om nødvendig samarbeide med Kommisjonen og de nasjonale vedkommende myndigheter under utøvelsen av deres kompetanse og myndighet i henhold til denne forordning.

4. Tilbydere av allsidige AI-modeller kan basere seg på retningslinjene for god praksis i henhold til artikkel 56 for å påvise samsvar med forpliktelsene fastsatt i nr. 1 i denne artikkel, inntil en harmonisert standard er offentliggjort. Overholdelse av europeiske harmoniserte standarder gir tilbydere en formodning om samsvar i den utstrekning disse standardene dekker disse forpliktelsene. Tilbydere AV AI-modeller til allmenn bruk som ikke følger en godkjent praksis eller ikke en europeisk harmonisert standard, skal påvise alternative egnede metoder for samsvar for Kommisjonens vurdering.

5. For å lette overholdelsen av vedlegg XI, særlig . 2 bokstav d) og e), Kommisjonen myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 for å detaljere måle- og beregningsmetoder med sikte på å muliggjøre sammenlignbar og verifiserbar dokumentasjon.

6. Kommisjonen er gitt myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 nr. 2 for å endre vedlegg XI og XII i lys av den teknologiske utviklingen.

7. all informasjon eller dokumentasjon innhentet i henhold til denne artikkel, herunder forretningshemmeligheter, skal behandles i samsvar med konfidensialitetsforpliktelsene fastsatt i artikkel 78.

Artikkel 54

Autoriserte representanter for leverandører av generelle AI-modeller

1. Før leverandører som er etablert i tredjeland, markedsfører en allsidig AI-modell på unionsmarkedet, skal de ved skriftlig fullmakt utpeke en autorisert representant som er etablert i Unionen.

2. Tilbyderen skal gjøre det mulig for sin autoriserte representant å utføre de oppgavene som er spesifisert i fullmakten som er mottatt fra tilbyderen.

3. Den autoriserte representanten skal utføre de oppgavene som er angitt i fullmakten fra leverandøren. Den skal på anmodning gi en kopi av fullmakten til AI-kontoret på et av de offisielle språkene til Unionens institusjoner. Ved anvendelsen av denne forordning skal fullmakten gi den autoriserte representanten fullmakt til å utføre følgende oppgaver

(a) kontrollere at den tekniske dokumentasjonen angitt i vedlegg XI er utarbeidet, og at leverandøren har oppfylt alle forpliktelsene nevnt i artikkel 53 og, der det er relevant, artikkel 55;

(b) oppbevare en kopi av den tekniske dokumentasjonen som er spesifisert i vedlegg XI, slik at den står til rådighet for AI-KONTORET og nasjonale kompetente myndigheter i en periode på 10 år etter at aI-modellen til allmenn bruk er brakt i omsetning, samt kontaktopplysningene til leverandøren som har utpekt den autoriserte representanten;

(c) på begrunnet anmodning gi AI-kontoret all informasjon og dokumentasjon, herunder den som ER i bokstav b), som er nødvendig for å påvise at forpliktelsene i dette kapittel er oppfylt;

(d) samarbeide med aI-kontoret og vedkommende myndigheter, på begrunnet anmodning, i alle tiltak de treffer I forbindelse den generelle aI-modellen, herunder når modellen integreres I aI-systemer som bringes I omsetning eller tas i bruk i Unionen.

4. Fullmakten skal gi den autoriserte representanten rett til å bli kontaktet, i tillegg til ELLER I stedet for leverandøren, av AI-kontoret eller vedkommende myndigheter i alle spørsmål knyttet til å sikre overholdelse av denne forordning.

5. Den autoriserte representanten skal bringe fullmakten til opphør dersom den anser eller har grunn til å anse leverandøren opptrer i strid med sine forpliktelser i henhold til denne forordning. I slike tilfeller skal den også umiddelbart underrette AI-kontoret om oppsigelsen AV fullmakten og årsakene til dette.

6. Forpliktelsen fastsatt i denne artikkel får ikke anvendelse på leverandører av generelle aI-modeller som er utgitt under en gratis lisens med åpen kildekode som tillater tilgang, bruk, endring og distribusjon av modellen, og hvis parametere, herunder vektene, informasjonen om modellarkitekturen og informasjonen om modellbruk, gjøres offentlig tilgjengelig, med mindre de generelle AI-MODELLENE utgjør en systemrisiko.

AVSNITT 3

Forpliktelser for leverandører av generelle AI-modeller med systemrisiko

Artikkel 55

Forpliktelser for leverandører av generelle AI-modeller med systemrisiko

1. I tillegg til forpliktelsene oppført I artikkel 53 og 54, skal leverandører av generelle AI-modeller med systemrisiko

(a) utføre modellevaluering i samsvar med standardiserte protokoller og verktøy som gjenspeiler det nyeste innen teknologi, herunder gjennomføre og dokumentere kontradiktorisk testing av modellen med sikte på å identifisere og redusere systemrisiko;

(b) vurdere og redusere mulige systemiske risikoer på unionsnivå, herunder kildene til disse, som kan oppstå som følge av utvikling, markedsføring eller bruk av generelle KI-modeller med systemisk risiko;

(c) holde oversikt over, dokumentere og rapportere, uten unødig forsinkelse, til aI-kontoret og, der det er hensiktsmessig, til nasjonale kompetente myndigheter, relevant informasjon om alvorlige hendelser og mulige korrigerende tiltak for å håndtere dem;

(d) sikre et tilstrekkelig nivå av cybersikkerhetsbeskyttelse for den generelle aI-modellen med systemrisiko og modellens fysiske infrastruktur.

2. Tilbydere av generelle KI-modeller med systemrisiko kan basere seg på regler for god praksis i henhold til artikkel 56 for å påvise samsvar med forpliktelsene fastsatt i nr. 1 i denne artikkel, inntil en harmonisert standard er offentliggjort. Overholdelse av europeiske harmoniserte standarder gir tilbydere en presumsjon om samsvar i den grad disse standardene dekker disse forpliktelsene. Tilbydere av generelle KI-modeller med systemrisikoer som ikke følger en godkjent praksis eller ikke overholder en europeisk harmonisert standard, skal påvise alternative adekvate måter å overholde forpliktelsene på, slik at Kommisjonen kan vurdere dem.

3. all informasjon eller dokumentasjon innhentet i henhold til denne artikkel, herunder forretningshemmeligheter, skal behandles i samsvar med konfidensialitetsforpliktelsene fastsatt i artikkel 78.

AVSNITT 4

Retningslinjer for god praksis

Artikkel 56

Retningslinjer for god praksis

1. AI-kontoret skal oppmuntre til og legge til rette for at det utarbeides regler for god praksis på unionsplan for å bidra til en korrekt anvendelse av denne forordning, idet det tas hensyn til internasjonale tilnærminger.

2. AI-kontoret og styret skal ha som mål å sikre at de etiske retningslinjene minst dekker de forpliktelsene som ER fastsatt i artikkel 53 og 55, herunder følgende spørsmål

(a) midler for å sikre at informasjonen nevnt i artikkel 53 nr. 1 bokstav a) og b) holdes oppdatert i lys av den markedsmessige og teknologiske utviklingen;

(b) tilstrekkelig detaljnivå for sammendraget om innholdet som brukes til opplæring;

(c) identifisering av typen og arten av systemrisikoer på unionsnivå, herunder kildene til disse, der det er relevant;

(d) tiltak, framgangsmåter og ordninger for vurdering og håndtering av systemrisikoer på unionsplan, herunder dokumentasjon av disse, som skal stå i forhold til risikoene, ta hensyn til hvor alvorlige og sannsynlige de er, og ta hensyn til de særlige utfordringene ved å håndtere disse risikoene i lys av de mulige måtene slike risikoer kan oppstå og materialisere SEG PÅ I DEN INTERNE verdikjeden.

3. aI-kontoret kan invitere alle tilbydere av generelle aI-modeller, samt relevante nasjonale kompetente myndigheter, til å delta i utarbeidelsen av retningslinjer for god praksis. Organisasjoner i det sivile samfunn, næringslivet, akademia og andre relevante interessenter, for eksempel nedstrømsleverandører og uavhengige eksperter, kan støtte prosessen.

4. AI-kontoret og styret skal ha som mål å sikre at retningslinjene for god praksis klart fastsetter sine spesifikke mål og inneholder forpliktelser eller tiltak, herunder sentrale resultatindikatorer der det er hensiktsmessig, for å sikre at disse målene nås, og at de tar behørig hensyn til behovene og interessene til alle berørte parter, herunder berørte personer, på unionsnivå.

5. aI-kontoret skal ha som mål å sikre at deltakerne i de etiske retningslinjene regelmessig rapporterer til aI-kontoret om gjennomføringen av forpliktelsene og tiltakene som er truffet og resultatene av disse, herunder målt mot nøkkelindikatorene for resultater, der det er hensiktsmessig. Nøkkelindikatorene og rapporteringsforpliktelsene skal gjenspeile forskjeller i størrelse og kapasitet mellom de ulike deltakerne.

6. AI-kontoret og styret skal regelmessig overvåke og evaluere deltakernes oppnåelse av målene for retningslinjene for god praksis og deres bidrag til en korrekt anvendelse av denne forordning. AI-kontoret og styret skal vurdere om retningslinjene dekker forpliktelsene fastsatt I artikkel 53 og 55, og skal regelmessig overvåke og evaluere oppnåelsen av målene for dem. De skal offentliggjøre sin vurdering av hvorvidt retningslinjene tilstrekkelige.

Kommisjonen kan ved hjelp av en gjennomføringsrettsakt godkjenne en kodeks for god praksis og gi den generell gyldighet i Unionen. Denne gjennomføringsrettsakten skal vedtas i samsvar med undersøkelsesprosedyren nevnt i artikkel 98 nr. 2.

7. aI-kontoret kan oppfordre alle tilbydere av generelle aI-modeller til å slutte seg til . For tilbydere av generelle aI-modeller som ikke utgjør en systemrisiko, kan denne tilslutningen begrenses til forpliktelsene fastsatt i artikkel 53, med mindre de uttrykkelig erklærer at de er interessert i å slutte seg til den fullstendige kodeksen.

8. aI-kontoret skal også, der det er hensiktsmessig, oppmuntre til og legge til rette for gjennomgang tilpasning av retningslinjene, særlig i lys av nye standarder. AI-kontoret skal bistå i vurderingen av tilgjengelige standarder.

9. Retningslinjene skal være klare senest 2. mai 2025. AI-kontoret skal treffe de nødvendige tiltak, herunder invitere leverandører i henhold til nr. 7.

Dersom det innen 2. august 2025 ikke kan ferdigstilles en kodeks for god praksis, eller dersom AI-kontoret anser den som utilstrekkelig etter sin vurdering i henhold til nr. 6 i denne artikkel, kan Kommisjonen ved hjelp av gjennomføringsrettsakter fastsette felles regler for gjennomføringen forpliktelsene fastsatt I artikkel 53 og 55, herunder de spørsmålene som er angitt i nr. 2 i denne artikkel. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten for undersøkelse nevnt i artikkel 98 nr. 2.

CHaPTER VI

TILTAK TIL STØTTE FOR INNOVASJON

Artikkel 57

Regulatoriske sandkasser for kunstig intelligens

1. Medlemsstatene skal sikre at deres vedkommende myndigheter oppretter minst én regulatorisk sandkasse på nasjonalt plan, som skal være i drift innen 2. august 2026. Denne sandkassen kan også opprettes i fellesskap med vedkommende myndigheter i andre medlemsstater. Kommisjonen kan gi teknisk støtte, råd og verktøy for og drift av sandkasser for AI-regelverk.

Forpliktelsen etter første ledd kan også oppfylles ved å delta i en eksisterende sandkasse i den utstrekning denne deltakelsen gir et tilsvarende nivå av nasjonal dekning for de deltakende medlemsstatene.

2. Det kan også opprettes flere regulatoriske sandkasser på regionalt eller lokalt nivå, eller i samarbeid med vedkommende myndigheter i andre medlemsstater.

3. Den europeiske datatilsynsmann kan også opprette en regulatorisk sandkasse for Unionens institusjoner, organer, kontorer og byråer, og kan utøve de nasjonale vedkommende myndigheters roller og oppgaver i samsvar med dette kapittel.

4. Medlemsstatene skal sikre at vedkommende myndigheter nevnt i nr. 1 og 2 avsetter tilstrekkelige ressurser til å etterleve denne artikkel effektivt og til rett tid. Når det er hensiktsmessig, skal nasjonale vedkommende myndigheter samarbeide med andre relevante myndigheter og kan tillate at andre aktører I økosystemet FOR kunstig INTELLIGENS trekkes inn. Denne artikkel skal ikke berøre andre regulatoriske sandkasser som er etablert i henhold til unionsretten eller nasjonal rett. Medlemsstatene skal sikre et hensiktsmessig nivå av samarbeid mellom myndighetene som fører tilsyn med disse andre sandkassene, og de nasjonale vedkommende myndigheter.

5. Sandkasser for kunstig intelligens som er opprettet i henhold til nr. 1, skal sørge for et kontrollert miljø som fremmer innovasjon og legger til rette for utvikling, opplæring, testing og validering av innovative systemer for KUNSTIG INTELLIGENS I en begrenset periode før de bringes i omsetning eller tas i bruk i henhold til en spesifikk sandkasseplan som er avtalt mellom tilbyderne eller potensielle tilbydere og vedkommende myndighet. Slike sandkasser kan omfatte testing under reelle forhold som overvåkes der.

6. Vedkommende myndigheter skal, der det er hensiktsmessig, gi veiledning, tilsyn og støtte innenfor den INTERNASJONALE regulatoriske sandkassen med sikte på å identifisere risikoer, særlig for grunnleggende rettigheter, helse og sikkerhet, testing, risikoreduserende tiltak og deres effektivitet i forhold til forpliktelsene kravene i denne forordning og, der det er relevant, annen unionsrett og nasjonal rett som det føres tilsyn med innenfor sandkassen.

7. Kompetente myndigheter skal gi tilbydere og potensielle tilbydere som deltar i DEN regulatoriske sandkassen, veiledning om regulatoriske forventninger og om hvordan de skal oppfylle kravene og forpliktelsene fastsatt i denne forordning.

På anmodning fra leverandøren eller den potensielle leverandøren AV aI-systemet skal vedkommende myndighet fremlegge et skriftlig bevis på de vellykkede aktivitetene som er gjennomført i sandkassen. Vedkommende myndighet skal også fremlegge en avslutningsrapport med en detaljert beskrivelse av aktivitetene som er utført i sandkassen, og de tilhørende resultatene og læringsutbyttene. Tilbyderne kan bruke denne dokumentasjonen til å påvise at de overholder denne forordning gjennom samsvarsvurderingsprosessen eller relevante markedstilsynsaktiviteter. I denne forbindelse skal markedstilsynsmyndighetene og meldte organer ta positivt hensyn til avslutningsrapportene og det skriftlige beviset fra den nasjonale vedkommende myndighet, med sikte på å fremskynde framgangsmåtene for samsvarsvurdering i rimelig grad.

8. Med forbehold for bestemmelsene om konfidensialitet i artikkel 78, og med samtykke fra tilbyderen eller den potensielle , skal Kommisjonen og styret ha tilgang til utmeldingsrapportene og skal ta hensyn til dem, der det er relevant, når de utfører sine oppgaver i henhold til denne forordning. Dersom både tilbyderen eller den potensielle tilbyderen og den nasjonale vedkommende myndighet uttrykkelig samtykker, kan utmeldingsrapporten gjøres offentlig tilgjengelig gjennom den felles informasjonsplattformen nevnt i denne artikkel.

9. Etableringen AV en regulatorisk sandkasse skal bidra til å oppnå følgende mål

(a) forbedre rettssikkerheten for å oppnå samsvar med denne forordning eller, der det er relevant, annen gjeldende unionsrett og nasjonal rett;

(b) støtte deling av beste praksis gjennom samarbeid med myndighetene som er involvert i den regulatoriske sandkassen;

(c) fremme innovasjon og konkurranseevne og legge til rette for utvikling av ET AI-økosystem;

(d) bidra til kunnskapsbasert læring om regelverket;

(e) legge til rette for og fremskynde tilgangen til unionsmarkedet FOR AI-systemer, særlig når de leveres av små og mellomstore bedrifter, herunder oppstartsbedrifter.

10. Nasjonale vedkommende myndigheter skal, i utstrekning de innovative aI-systemene innebærer behandling av personopplysninger eller på annen måte faller inn under tilsynsområdet til andre nasjonale myndigheter eller vedkommende myndigheter som gir eller støtter tilgang til data, sikre at de nasjonale personvernmyndighetene og disse andre nasjonale eller myndighetene er tilknyttet driften AV DEN aI-regulatoriske sandkassen og deltar i tilsynet med disse aspektene I DEN utstrekning deres respektive oppgaver og fullmakter det.

11. De regulatoriske sandkassene skal ikke påvirke tilsyns- eller korrigeringsbeføyelsene til vedkommende myndigheter som fører tilsyn med sandkassene, herunder på regionalt eller lokalt nivå. eventuelle betydelige risikoer for helse, miljø og sikkerhet og grunnleggende rettigheter som identifiseres under utviklingen og testingen av slike aI-systemer, skal føre til tilstrekkelige avbøtende tiltak. Nasjonale vedkommende myndigheter skal ha myndighet til midlertidig eller permanent å stanse testprosessen eller deltakelsen I sandkassen dersom det ikke er mulig å avbøte risikoen på en effektiv måte, og skal underrette aI-kontoret om en slik beslutning. Nasjonale vedkommende myndigheter skal utøve sin tilsynsmyndighet innenfor rammene av den relevante lovgivningen og bruke sin skjønnsmessige myndighet når de gjennomfører rettslige bestemmelser med hensyn til et spesifikt sandkasseprosjekt for AI-regulering, med sikte på å støtte innovasjon innen AI i Unionen.

12. Tilbydere og potensielle tilbydere som deltar i DEN regulatoriske sandkassen for AI, skal fortsatt være ansvarlige i henhold til gjeldende unionsrett og nasjonal ansvarslovgivning for enhver skade som påføres tredjeparter som følge av eksperimenteringen som finner sted i sandkassen. Forutsatt at de potensielle tilbyderne overholder den særskilte planen og vilkårene og betingelsene for sin deltakelse og i god tro følger veiledningen fra den nasjonale vedkommende myndighet, skal myndighetene imidlertid ikke ilegge administrative bøter for brudd på denne forordning. Dersom andre vedkommende myndigheter med ansvar for annen unionsrett og nasjonal rett var aktivt involvert i tilsynet med aI-systemet i sandkassen og ga veiledning om etterlevelse, skal det ikke ilegges administrative bøter med hensyn til denne retten.

13. De internasjonale regulatoriske sandkassene skal utformes og gjennomføres på en slik måte at de, der det er relevant, legger til rette for samarbeid over landegrensene mellom nasjonale vedkommende myndigheter.

14. Nasjonale kompetente myndigheter skal samordne sine aktiviteter og samarbeide innenfor rammen av nemnda.

15. Nasjonale vedkommende myndigheter skal informere aI-kontoret og styret om opprettelsen av en sandkasse, og kan be dem om støtte og veiledning. aI-kontoret skal offentliggjøre en liste over planlagte og eksisterende sandkasser og holde den oppdatert å oppmuntre til mer samhandling i de regulatoriske sandkassene og samarbeid på tvers av landegrensene.

16. Nasjonale vedkommende myndigheter skal framlegge årlige rapporter for AI-KONTORET og styret, fra ett år etter opprettelsen av den regulatoriske sandkassen og deretter hvert år fram til den avsluttes, samt en sluttrapport. Disse rapportene skal gi informasjon om framdriften og resultatene av gjennomføringen av disse sandkassene, herunder beste praksis, hendelser, erfaringer anbefalinger om opprettelsen av dem og, der det er relevant, om anvendelsen og en eventuell revisjon av denne forordning, herunder dens delegerte rettsakter og gjennomføringsrettsakter, og om anvendelsen av annen unionsrett som vedkommende myndigheter fører tilsyn med i sandkassen. De nasjonale vedkommende myndigheter skal gjøre disse årsrapportene eller sammendrag av dem tilgjengelige for allmennheten på nettet. Kommisjonen skal, der det er relevant, ta hensyn til årsrapportene når den utøver sine oppgaver i henhold til denne forordning.

17. Kommisjonen skal utvikle et enkelt og dedikert grensesnitt som inneholder all relevant informasjon knyttet til aI-regulatoriske sandkasser, slik at interessenter kan samhandle med aI-regulatoriske sandkasser og rette forespørsler til vedkommende myndigheter, og søke ikke-bindende veiledning om samsvar for innovative produkter, tjenester og forretningsmodeller som omfatter aI-teknologi, i samsvar med artikkel 62 nr. 1 bokstav c). Kommisjonen skal proaktivt samordne med nasjonale vedkommende myndigheter, der det er relevant.

Artikkel 58

Detaljerte ordninger for, og regulatoriske sandkasser for kunstig intelligens fungerer

1. For å unngå fragmentering i Unionen skal Kommisjonen vedta gjennomføringsrettsakter som spesifiserer de nærmere ordningene for opprettelse, utvikling, gjennomføring, drift og tilsyn med DE internasjonale regulatoriske sandkassene. Gjennomføringsrettsaktene skal omfatte felles prinsipper om følgende spørsmål:

(a) kriterier for kvalifisering og utvelgelse for deltakelse i den regulatoriske sandkassen;

(b) prosedyrer for søknad, deltakelse, overvåking, avslutning og avslutning av den regulatoriske sandkassen, inkludert sandkasseplanen og avslutningsrapporten;

(c) vilkårene og betingelsene som gjelder for deltakerne.

Disse gjennomføringsrettsaktene skal vedtas i samsvar med undersøkelsesprosedyren nevnt i artikkel 98 nr. 2.

2. Gjennomføringsrettsaktene nevnt i nr. 1 skal sikre

(a) at sandkasser for aI-regulering er åpne for alle tilbydere eller potensielle tilbydere AV ET aI-system som oppfyller kvalifiserings- og utvelgelseskriteriene, som skal være åpne og rettferdige, og at nasjonale kompetente myndigheter informerer søkerne om sin beslutning innen tre måneder etter at søknaden er mottatt;

(b) at de regulatoriske sandkassene gir bred og lik tilgang og holder tritt med etterspørselen etter deltakelse; tilbydere og potensielle tilbydere kan også sende inn søknader i partnerskap med distributører og andre relevante tredjeparter;

(c) at de nærmere ordningene for og vilkårene for sandkasser for AI-regelverk i størst mulig grad gir nasjonale vedkommende myndigheter fleksibilitet til å opprette og drive sine sandkasser for AI-regelverk;

(d) at tilgang til de regulatoriske sandkassene er gratis for små og mellomstore bedrifter, herunder nyetablerte bedrifter, med forbehold for ekstraordinære kostnader som nasjonale vedkommende myndigheter kan kreve dekket på en rettferdig og forholdsmessig måte;

(e) at de ved hjelp av læringsresultatene fra de regulatoriske sandkassene gjør det lettere for tilbydere og potensielle tilbydere å oppfylle samsvarsvurderingsforpliktelsene i henhold til denne forordning og den frivillige anvendelsen av de etiske retningslinjene nevnt i artikkel 95;

(f) at sandkasser for AI-regelverk legger til rette for involvering av andre relevante aktører I AI-økosystemet, som meldte organer og standardiseringsorganisasjoner, små og mellomstore bedrifter, herunder oppstartsbedrifter, foretak, innovatører, test- og forsøksfasiliteter, forsknings- og forsøkslaboratorier og europeiske knutepunkter for digital innovasjon, sentre for fremragende forskning og individuelle forskere, for å muliggjøre og legge til rette for samarbeid med offentlig og privat sektor;

(g) at framgangsmåter, prosesser og administrative krav for søknad, utvelgelse, deltakelse og avslutning av en sandkasse for AI-regulering er enkle, lett forståelige og tydelig kommunisert for å gjøre det lettere for små og mellomstore bedrifter, herunder nyetablerte bedrifter, med begrenset juridisk og administrativ kapasitet å delta, og at de ER strømlinjeformet I hele Unionen for å unngå fragmentering, og at deltakelse i en sandkasse for AI-regulering som er opprettet av en medlemsstat eller av Den europeiske datatilsynsmann, anerkjennes gjensidig og på en ensartet måte og har samme rettsvirkninger I hele Unionen;

(h) at deltakelse i DEN regulatoriske sandkassen er begrenset en periode som er tilpasset prosjektets kompleksitet og omfang, og som kan forlenges av den nasjonale kompetente myndigheten;

(i) at sandkasser for AI-regulering legger til rette for utvikling av verktøy og infrastruktur for testing, benchmarking, vurdering og forklaring av dimensjoner ved AI-systemer som er relevante for reguleringslæring, for eksempel nøyaktighet, robusthet og cybersikkerhet, samt tiltak for å redusere risiko for grunnleggende rettigheter og samfunnet som helhet.

3. Potensielle tilbydere I de regulatoriske sandkassene FOR AI, særlig små og mellomstore bedrifter og oppstartsbedrifter, skal, der det er relevant, henvises til tjenester før innføring, f.eks. veiledning om gjennomføringen av denne forordning, til andre verdiøkende tjenester, f.eks. hjelp med standardiseringsdokumenter og sertifisering, test- og forsøksfasiliteter, europeiske digitale innovasjonssentre og sentre for fremragende forskning.

4. Dersom nasjonale vedkommende myndigheter vurderer å tillate utprøving under reelle forhold under tilsyn innenfor rammen av en regulatorisk sandkasse FOR KUNSTIG INTELLIGENS SOM skal opprettes i henhold til denne artikkel, skal de særlig avtale vilkårene og betingelsene for slik utprøving og særlig hensiktsmessige sikkerhetstiltak med deltakerne, med sikte på å verne grunnleggende rettigheter, helse og sikkerhet. Der det er hensiktsmessig, skal de samarbeide med andre nasjonale vedkommende myndigheter med sikte på å sikre ensartet praksis i hele Unionen.

Artikkel 59

Videre behandling av personopplysninger for å utvikle visse AI-systemer i allmennhetens interesse i den regulatoriske AI-sandkassen

1. I den regulatoriske sandkassen kan personopplysninger som er lovlig innsamlet for andre formål, behandles utelukkende med det formål å utvikle, lære opp og teste visse aI-systemer i sandkassen når alle de følgende vilkårene er oppfylt:

(a) aI-systemer skal utvikles for å ivareta vesentlige samfunnsinteresser av en offentlig myndighet eller en annen fysisk eller juridisk person og på ett eller flere av følgende områder

(i) offentlig sikkerhet og folkehelse, inkludert sykdomsoppdagelse, diagnose, forebygging, kontroll og behandling og forbedring av helsevesenet;

(ii) et høyt nivå av beskyttelse og forbedring av miljøkvaliteten, beskyttelse av biologisk mangfold, mot forurensning, tiltak for grønn omstilling og tiltak for å redusere og tilpasse seg klimaendringene;

(iii) bærekraftig energi;

(iv) sikkerhet og robusthet i transportsystemer og mobilitet, kritisk infrastruktur og nettverk;

(v) effektivitet og kvalitet i offentlig forvaltning og offentlige tjenester;

(b) de behandlede opplysningene er nødvendige for å oppfylle ett eller flere av kravene nevnt i kapittel III, avsnitt 2, dersom disse kravene ikke kan oppfylles effektivt ved behandling av anonymiserte, syntetiske eller andre ikke-personlige opplysninger;

(c) det finnes effektive overvåkingsmekanismer for å identifisere om det kan oppstå høy risiko for de registrertes rettigheter og friheter, som nevnt i artikkel 35 i forordning (EU) 2016/679 og i artikkel 39 i forordning (EU) 2018/1725, under sandkasseeksperimenteringen, samt reaksjonsmekanismer for raskt å redusere disse risikoene og, om nødvendig, stanse behandlingen;

(d) alle personopplysninger som skal behandles i forbindelse med sandkassen, befinner seg i et funksjonelt separat, isolert og beskyttet databehandlingsmiljø under potensielle leverandørens kontroll, og bare autoriserte personer har tilgang disse opplysningene;

(e) Tilbydere kan kun dele de opprinnelig innsamlede dataene videre i samsvar med EUs personvernlovgivning. Personopplysninger som er opprettet i sandkassen, kan ikke deles utenfor sandkassen;

(f) enhver behandling av personopplysninger i forbindelse med sandkassen verken fører til tiltak eller beslutninger som påvirker de registrerte, eller påvirker anvendelsen av deres rettigheter fastsatt i unionsretten om vern av personopplysninger;

(g) alle personopplysninger som behandles i forbindelse med sandkassen, beskyttes ved hjelp av egnede tekniske og organisatoriske tiltak og slettes når deltakelsen i sandkassen er avsluttet eller personopplysningene har nådd slutten av oppbevaringsperioden;

(h) loggene over behandlingen av personopplysninger i forbindelse med sandkassen oppbevares så lenge deltakelsen i sandkassen varer, med mindre annet er fastsatt i unionsretten eller nasjonal rett;

(i) en fullstendig og detaljert beskrivelse av prosessen og begrunnelsen for opplæringen, testingen og valideringen AV KI-systemet oppbevares sammen med testresultatene som en del av tekniske dokumentasjonen som det henvises til i vedlegg IV;

(j) et kort sammendrag AV aI-prosjektet som er utviklet i sandkassen, dets mål og forventede resultater, offentliggjøres på nettstedet til vedkommende myndigheter. denne forpliktelsen skal ikke omfatte sensitive operative data i forbindelse med virksomheten til rettshåndhevelses-, grensekontroll-, innvandrings- eller asylmyndigheter.

2. Med henblikk på å forebygge, etterforske, avsløre eller straffeforfølge straffbare handlinger eller fullbyrde strafferettslige sanksjoner, herunder beskytte mot og forebygge trusler mot offentlige sikkerhet, under rettshåndhevelsesmyndighetenes kontroll og ansvar, skal behandlingen av personopplysninger i EN regulatorisk sandkasse være basert en bestemt unionsrett eller nasjonal rett og underlagt de samme kumulative vilkårene som nevnt i nr. 1.

3. Nr. 1 berører ikke unionsretten eller nasjonal rett som utelukker behandling av personopplysninger for andre formål enn dem som uttrykkelig er nevnt i nevnte rett, og heller ikke unionsretten eller nasjonal rett som fastsetter grunnlaget for behandling av personopplysninger som er nødvendig for utvikling, utprøving eller opplæring av innovative KI-systemer eller ethvert annet rettslig grunnlag, i samsvar med unionsretten om vern av personopplysninger.

Artikkel 60

Testing av høyrisikosystemer for kunstig intelligens under reelle forhold utenfor AI-regulatoriske sandkasser

1. Leverandører eller potensielle leverandører av høYRISIKO-AI-SYSTEMER oppført i vedlegg III kan gjennomføre testing av høyrisiko-AI-systemer under reelle forhold utenfor sandkasser med regelverk, i samsvar med denne artikkel og planen for testing i den virkelige verden nevnt i denne artikkel, uten at det berører forbudene I henhold til artikkel 5.

Kommisjonen skal ved hjelp av gjennomføringsrettsakter fastsette de nærmere elementene i planen for utprøving i den virkelige verden. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten for undersøkelse nevnt i artikkel 98 nr. 2.

Dette ledd skal ikke berøre unionsretten eller nasjonal lovgivning om prøving under reelle forhold av høyrisikosystemer knyttet til produkter som omfattes av Unionens harmoniseringsregelverk oppført i vedlegg I.

2. Tilbydere eller potensielle tilbydere kan gjennomføre testing av høyrisikosystemer for kunstig INTELLIGENS som nevnt i vedlegg III under reelle forhold når som helst før de bringer systemet for KUNSTIG INTELLIGENS I omsetning eller tar det i bruk, enten på egen hånd eller i samarbeid med en eller flere ibruktakere eller potensielle ibruktakere.

3. Utprøving av høyrisiko-AI-systemer under reelle forhold i henhold til denne artikkelen skal ikke berøre eventuelle etiske vurderinger som kreves i henhold til unionsretten eller nasjonal rett.

4. Tilbydere eller potensielle tilbydere kan kun utføre testingen under reelle forhold dersom alle følgende vilkår er oppfylt:

(a) leverandøren eller den potensielle leverandøren har utarbeidet en plan for testing i den virkelige verden og sendt den inn til markedstilsynsmyndigheten i den medlemsstaten der testingen i den virkelige verden skal gjennomføres;

(b) markedstilsynsmyndigheten i medlemsstaten der testingen under reelle forhold skal gjennomføres, har godkjent under reelle forhold og planen for testing under reelle forhold; dersom markedstilsynsmyndigheten ikke har gitt svar innen 30 dager, skal testingen under reelle forhold og planen for testing under reelle forhold anses for å være godkjent; dersom nasjonal lovgivning ikke åpner for en stilltiende godkjenning, skal testingen under reelle forhold fortsatt være underlagt krav om tillatelse;

(c) leverandøren eller den potensielle leverandøren, med unntak av leverandører eller potensielle leverandører av nevnt i nr. 1, 6 og 7 i vedlegg III på områdene rettshåndhevelse, migrasjon, asyl og grensekontrollforvaltning, og HØYRISIKO-AI-SYSTEMER nevnt i nr. 2 i vedlegg III, har registrert utprøvingen under reelle forhold i samsvar med artikkel 71 nr. 4 med et unionsomfattende unikt felles identifikasjonsnummer og med opplysningene angitt i vedlegg IX; leverandøren eller den potensielle leverandøren AV høyrisiko-AI-systemer nevnt i nr. 1, 6 og 7 i vedlegg III områdene rettshåndhevelse, migrasjon, asyl og , har registrert testingen under reelle forhold i den sikre ikke-offentlige delen av EU-databasen i samsvar med artikkel 49 nr. 4 bokstav d), med et unionsomfattende unikt felles identifikasjonsnummer og med opplysningene som er angitt der; leverandøren eller den potensielle leverandøren av høyrisiko-AI-systemer nevnt i nr. 2 I vedlegg III har registrert testingen under reelle forhold i samsvar med artikkel 49 nr. 5;

(d) tilbyderen eller den potensielle tilbyderen utfører testingen under reelle forhold, er etablert i Unionen eller har utpekt en juridisk representant som er etablert i Unionen;

(e) Data som samles inn og behandles med henblikk på testing under reelle forhold, skal bare overføres til tredjestater under forutsetning av at egnede og gjeldende garantier i henhold til unionsretten er gjennomført;

(f) testingen under reelle forhold ikke varer lenger enn det som er nødvendig for å nå målene, og i alle tilfeller ikke lenger enn seks måneder, som kan forlenges med ytterligere seks måneder, forutsatt at tilbyderen eller den potensielle tilbyderen på forhånd har underrettet markedstilsynsmyndigheten om dette, sammen med en forklaring på behovet for en slik forlengelse;

(g) Testpersonene som testes under reelle forhold, og som tilhører sårbare grupper på grunn av alder eller funksjonshemming, er tilstrekkelig beskyttet;

(h) dersom en tilbyder eller potensiell tilbyder organiserer utprøving under reelle forhold i samarbeid med en eller flere ibruktakere eller potensielle ibruktakere, skal sistnevnte ha blitt informert om alle aspekter ved utprøvingen som er relevante for deres beslutning om å delta, og ha fått de relevante instruksjonene for bruk AV KI-systemet nevnt i artikkel 13; tilbyderen eller den potensielle tilbyderen og IBRUKTAKEREN eller den potensielle ibruktakeren skal inngå en avtale som spesifiserer deres roller og ansvarsområder med sikte på å sikre samsvar med bestemmelsene for utprøving under reelle forhold i henhold til denne forordning og i henhold til annen gjeldende unionsrett og nasjonal rett.

(i) forsøkspersonene i testingen under reelle forhold har gitt informert samtykke I samsvar med artikkel 61, eller i tilfelle av rettshåndhevelse, der innhenting av informert samtykke vil forhindre at KI-systemet testes, skal selve testingen og resultatet av testingen under reelle forhold ikke ha noen negativ innvirkning på forsøkspersonene, og personopplysningene deres skal slettes etter at testen er utført;

(j) testingen under reelle forhold overvåkes effektivt av leverandøren eller den potensielle leverandøren, samt av utplasserere eller potensielle utplasserere gjennom personer som er tilstrekkelig kvalifisert på det relevante området og har den nødvendige kapasitet, opplæring og myndighet til å utføre sine oppgaver;

(k) kan spådommene, anbefalingene eller beslutningene fra AI-systemet I praksis reverseres og ignoreres.

5. alle forsøkspersoner som deltar i testingen under reelle forhold, eller deres lovlig utpekte representant, kan når som helst trekke seg fra testingen ved å tilbakekalle sitt informerte samtykke, uten at dette medfører skade og uten å måtte gi noen begrunnelse, og kan be om umiddelbar og permanent sletting av personopplysningene sine. Tilbaketrekking av det informerte samtykket skal ikke påvirke de aktivitetene som allerede er utført.

6. I samsvar med artikkel 75 skal medlemsstatene gi sine markedstilsynsmyndigheter myndighet til å kreve at tilbydere og potensielle tilbydere framlegger opplysninger, til å gjennomføre uanmeldte fjerninspeksjoner eller inspeksjoner på stedet og til å kontrollere gjennomføringen av testingen under reelle forhold og de tilknyttede høyrisikosystemene FOR KUNSTIG INTELLIGENS. Markedstilsynsmyndighetene skal bruke disse fullmaktene til å sikre en trygg utvikling av testing under reelle forhold.

7. skal enhver alvorlig hendelse som avdekkes i løpet av testingen under reelle forhold, rapporteres til den nasjonale markedstilsynsmyndigheten i samsvar med artikkel 73. Tilbyderen eller den potensielle tilbyderen skal treffe umiddelbare risikoreduserende tiltak eller, dersom dette ikke er mulig, innstille testingen under reelle forhold inntil slike risikoreduserende tiltak er , eller på annen måte avslutte den. Tilbyderen eller den potensielle tilbyderen skal etablere en prosedyre for umiddelbar tilbakekalling AV AI-systemet ved slik avslutning av testingen UNDER reelle forhold.

8. Tilbydere eller potensielle tilbydere skal underrette den nasjonale markedstilsynsmyndigheten i den medlemsstaten der testingen under reelle forhold skal gjennomføres, om at testingen under reelle forhold avbrytes eller avsluttes, og om de endelige resultatene.

9. Leverandøren eller den potensielle leverandøren skal være ansvarlig i henhold til gjeldende EU-rett og nasjonal ansvarslovgivning for enhver skade som forårsakes i løpet av testingen under reelle forhold.

Artikkel 61

Informert samtykke til å delta i testing under reelle forhold utenfor AI-regulatoriske sandkasser

1. For testing under reelle forhold i henhold til artikkel 60 skal det innhentes frivillig informert samtykke fra testpersonene før de deltar i slik testing, og etter at de er blitt behørig informert med kortfattet, klar, relevant og forståelig informasjon om:

(a) testens art og formål under reelle forhold og de mulige ulempene som kan være forbundet med deltakelsen;

(b) under hvilke forhold testingen i den virkelige verden skal gjennomføres, herunder forventet varighet av forsøkspersonens eller forsøkspersonenes deltakelse;

(c) deres rettigheter og garantiene for deres deltakelse, særlig deres rett til å nekte å delta i, og retten til å trekke seg fra, testing under reelle forhold når som helst, uten at det medfører noen skade og uten å måtte gi noen begrunnelse;

(d) ordningene for å be om reversering eller tilsidesettelse av spådommer, anbefalinger eller beslutninger fra AI-systemet;

(e) det unionsomfattende unike identifikasjonsnummeret for testingen under reelle forhold i samsvar med artikkel 60 nr. 4 c), og kontaktopplysningene til leverandøren eller dennes juridiske representant som ytterligere informasjon kan innhentes fra.

2. Det informerte samtykket skal dateres og dokumenteres, og en kopi skal gis til testpersonene eller deres juridiske representant.

Artikkel 62

Tiltak for leverandører og distributører, særlig små og mellomstore bedrifter, inkludert oppstartsbedrifter

1. Medlemsstatene skal iverksette følgende tiltak:

(a) gi små og mellomstore bedrifter, herunder nyetablerte foretak, som har et registrert kontor eller en filial I Unionen, prioritert tilgang til de regulatoriske sandkassene, i den utstrekning de oppfyller vilkårene for berettigelse og utvelgelseskriteriene; den prioriterte tilgangen skal ikke utelukke små og mellomstore bedrifter, herunder nyetablerte foretak, enn dem som ER nevnt i dette nummer, fra tilgang til den regulatoriske sandkassen, forutsatt at de også oppfyller vilkårene for berettigelse og utvelgelseskriteriene;

(b) organisere spesifikke bevisstgjørings- og opplæringsaktiviteter om anvendelsen av denne forordningen som er skreddersydd for små og mellomstore bedrifters behov, herunder nyetablerte bedrifter, utbyggere og, der det er hensiktsmessig, lokale offentlige myndigheter;

(c) bruke eksisterende dedikerte kanaler og, der det er hensiktsmessig, etablere nye kanaler for kommunikasjon med SMB-er, herunder oppstartsbedrifter, distributører, andre innovatører og, der det er hensiktsmessig, lokale offentlige myndigheter, for å gi råd og svare på spørsmål om gjennomføringen av denne forordningen, herunder om deltakelse i en regulatorisk sandkasse;

(d) legge til rette at små og mellomstore bedrifter og andre relevante interessenter kan delta i standardiseringsprosessen.

2. Det skal tas hensyn til de særlige interessene og behovene til SMB-tilbydere, herunder nyetablerte foretak, når gebyrene for samsvarsvurdering i henhold til artikkel 43 fastsettes, og disse gebyrene skal reduseres i forhold til deres størrelse, markedsstørrelse og andre relevante indikatorer.

3. AI-kontoret skal iverksette følgende tiltak:

(a) tilby standardiserte maler for områder som omfattes av denne forskriften, som spesifisert av styret i sin anmodning;

(b) utvikle og vedlikeholde en felles informasjonsplattform som gir brukervennlig informasjon om denne forordningen til alle operatører i hele Unionen;

(c) organisere egnede kommunikasjonskampanjer for å øke bevisstheten om forpliktelsene som følger av denne forordningen;

(d) evaluere og fremme konvergens AV beste praksis i offentlige anskaffelsesprosedyrer I forhold til AI-systemer.

Artikkel 63

Unntak for spesifikke operatører

1. Mikroforetak i henhold til rekommandasjon 2003/361/EF kan oppfylle visse deler av kvalitetsstyringssystemet som kreves i henhold til artikkel 17 i denne forordning, på en forenklet måte, forutsatt at de ikke har partnerforetak eller tilknyttede foretak i henhold til nevnte rekommandasjon. For dette formål skal Kommisjonen utarbeide retningslinjer for hvilke elementer i kvalitetsstyringssystemet som kan etterleves på en forenklet måte, idet det tas hensyn til mikroforetakenes behov, uten at det påvirker beskyttelsesnivået eller behovet for å oppfylle kravene til høyrisikosystemer.

2. Nr. 1 i denne artikkel skal ikke tolkes slik at disse driftsansvarlige fritas fra å oppfylle andre krav eller forpliktelser fastsatt i denne forordning, herunder de som er fastsatt i artikkel 9, 10, 11, 12, 13, 14 og 15,
72 og 73.

CHaPTER VII

STYRING

AVSNITT 1

Styring på unionsnivå

Artikkel 64

AI Office

1. Kommisjonen skal utvikle Unionens ekspertise og kapasitet på KI-området gjennom KI-kontoret.

2. Medlemsstatene skal legge til rette for de oppgavene som ER tillagt AI-kontoret, slik det fremgår av denne forordning.

Artikkel 65

Opprettelse og struktur for European Artificial Intelligence Board

1. Det opprettes herved ET europeisk styre for kunstig intelligens (styret").

2. Styret skal bestå av én representant fra hver . Den europeiske datatilsynsmann skal delta som observatør. Personvernkontoret skal også delta på styrets møter, men uten å delta i avstemningene. Andre nasjonale myndigheter og unionsmyndigheter, organer eller eksperter kan inviteres til møtene av styret fra sak til sak, dersom sakene som drøftes, er relevante for dem.

3. Hver representant skal utpekes av sin medlemsstat for en periode på tre år, som kan fornyes én gang.

4. Medlemsstatene skal sørge for at deres representanter i styret:

(a) ha relevant kompetanse og myndighet i sin medlemsstat, slik at de kan bidra aktivt til å utføre styrets oppgaver som nevnt i artikkel 66;

(b) utpekes som et felles kontaktpunkt overfor styret og, der det er hensiktsmessig, under hensyntagen til behov, som et felles kontaktpunkt for interessenter;

(c) har myndighet til å legge til rette for konsekvens og samordning mellom nasjonale vedkommende myndigheter i sin med hensyn til gjennomføringen av denne forordning, herunder gjennom innsamling av relevante data og opplysninger for å kunne utføre sine oppgaver i styret.

5. De utpekte representantene for medlemsstatene skal vedta styrets forretningsorden med to tredjedels flertall. Forretningsordenen skal særlig fastsette prosedyrer for utvelgelsesprosessen, varigheten av lederens mandat og spesifikasjoner av lederens oppgaver, detaljerte ordninger for avstemning og organiseringen av styrets og undergruppenes virksomhet.

6. Styret skal opprette to faste undergrupper som skal fungere som en plattform for samarbeid og utveksling mellom markedsovervåkingsmyndigheter og notifiserende myndigheter om spørsmål knyttet til henholdsvis markedsovervåking og notifiserte organer.

Den stående undergruppen for markedstilsyn bør fungere som administrativ samarbeidsgruppe (ADCO) for denne forordning i henhold til artikkel 30 i forordning (EU) 2019/1020.

Styret kan opprette andre faste eller midlertidige undergrupper etter behov for å behandle særlige spørsmål. Når det er hensiktsmessig, kan representanter for det rådgivende forumet nevnt i artikkel 67 inviteres til slike undergrupper eller til bestemte møter i disse undergruppene som observatører.

7. Styret skal organiseres og drives på en slik måte at objektivitet og upartiskhet i styrets virksomhet ivaretas.

8. Styret skal ledes av en av medlemsstatenes representanter. AI-kontoret skal ivareta sekretariatsfunksjonen for styret, innkalle til møtene etter anmodning fra styrelederen og utarbeide dagsorden i samsvar med styrets oppgaver i henhold til denne forordning og dets forretningsorden.

Artikkel 66

Styrets oppgaver

Styret skal gi råd til og bistå Kommisjonen og medlemsstatene for å legge til rette for en konsekvent og effektiv anvendelse av denne forordning. For dette formål kan styret særlig

(a) bidra til samordningen mellom nasjonale vedkommende myndigheter med ansvar for anvendelsen av denne forordning og, i samarbeid og med forbehold for samtykke fra de berørte markedstilsynsmyndighetene, støtte felles aktiviteter for markedstilsynsmyndighetene nevnt i artikkel 74 nr. 11;

(b) samle og dele teknisk og regulatorisk ekspertise og beste praksis mellom medlemsstatene;

(c) gi råd om gjennomføringen av denne forordning, særlig når det gjelder håndhevelsen av reglene om generelle aI-modeller;

(d) bidra til harmonisering av administrativ praksis i medlemsstatene, herunder i forbindelse med unntak fra framgangsmåtene for samsvarsvurdering nevnt I artikkel 46, funksjonen til en regulatorisk sandkasse og utprøving under reelle forhold nevnt I artikkel 57, 59 og 60;

(e) på anmodning fra Kommisjonen eller på eget initiativ avgi anbefalinger og skriftlige uttalelser om alle relevante spørsmål knyttet til gjennomføringen av denne forordning og til en konsekvent og effektiv anvendelse av den, herunder

(i) om utvikling og anvendelse av atferdsnormer og regler for god forretningsskikk i henhold til denne forordning, av Kommisjonens retningslinjer;

(ii) evalueringen og gjennomgangen av denne forordning i henhold til artikkel 112, herunder med hensyn til rapportene om alvorlige hendelser nevnt i artikkel 73, og driften EU-databasen nevnt i artikkel 71, utarbeidelsen av de delegerte rettsaktene eller gjennomføringsrettsaktene, og med hensyn til mulige tilpasninger av denne forordning til Unionens harmoniseringsregelverk oppført i vedlegg I;

(iii) på tekniske spesifikasjoner eller eksisterende standarder med hensyn til kravene i kapittel III, avsnitt 2;

(iv) om bruk av harmoniserte standarder eller felles spesifikasjoner som nevnt i artikkel 40 og 41;

(v) trender, som europeisk global konkurranseevne innen AI, utbredelsen AV AI i unionen og utviklingen av digitale ferdigheter;

(vi) trender i utviklingen av typologien FOR INTERNASJONALE verdikjeder, og særlig hvilke konsekvenser dette har for ansvarliggjøring;

(vii) om det potensielle behovet for endring av vedlegg III i samsvar med artikkel 7, og om det potensielle behovet for en eventuell revisjon av artikkel 5 i henhold til artikkel 112, idet det tas hensyn til relevant tilgjengelig dokumentasjon og den siste teknologiske utviklingen;

(f) støtte kommisjonen i arbeidet med å fremme KUNNSKAP OM AI, offentlig bevissthet og forståelse av fordelene, risikoene, sikkerhetstiltakene og rettighetene og pliktene i forbindelse med bruk AV aI-systemer;

(g) legge til rette for utvikling av felles kriterier og en felles forståelse blant markedsoperatører og vedkommende myndigheter av de relevante begrepene som er fastsatt i denne forordning, herunder ved å bidra til utviklingen av referanseverdier;

(h) samarbeide, der det er hensiktsmessig, med andre unionsinstitusjoner, -organer, -kontorer og -byråer samt relevante ekspertgrupper og -nettverk i Unionen, særlig på områdene produktsikkerhet, cybersikkerhet, konkurranse, digitale tjenester og medietjenester, finansielle tjenester, forbrukervern, databeskyttelse og beskyttelse av grunnleggende rettigheter;

(i) bidra til et effektivt samarbeid med kompetente myndigheter i tredjeland og med internasjonale organisasjoner;

(j) bistå nasjonale vedkommende myndigheter og Kommisjonen med å utvikle den organisatoriske og tekniske ekspertisen som kreves for gjennomføringen av denne forordning, herunder ved å bidra til vurderingen av opplæringsbehovene for ansatte i medlemsstatene som er involvert i gjennomføringen av denne forordning;

(k) bistå AI-kontoret med å støtte nasjonale kompetente myndigheter i etableringen og utviklingen av AI-REGULATORISKE sandkasser, og legge til rette for samarbeid og informasjonsutveksling mellom AI-regulatoriske sandkasser;

(l) bidra til, og gi relevante råd om, utviklingen av veiledningsdokumenter;

(m) gi råd til Kommisjonen i internasjonale spørsmål om AI;

(n) gi uttalelser til Kommisjonen om de kvalifiserte varslene om generelle AI-modeller;

(o) motta uttalelser fra medlemsstatene om kvalifiserte varsler om generelle aI-modeller, og om nasjonale erfaringer og praksis når det gjelder overvåking og håndheving av aI-systemer, særlig systemer som integrerer de generelle aI-modellene.

Artikkel 67

Rådgivende forum

1. skal det opprettes et rådgivende forum som skal bidra med teknisk ekspertise og gi råd til styret og Kommisjonen, og bidra til deres oppgaver i henhold til denne forordning.

2. Medlemmene av det rådgivende forumet skal representere et balansert utvalg av interessenter, herunder næringslivet, nyetablerte foretak, små og mellomstore bedrifter, det sivile samfunn og den akademiske verden. Sammensetningen av det rådgivende forumet skal være balansert med hensyn til kommersielle og ikke-kommersielle interesser og, innenfor kategorien kommersielle interesser, med hensyn til små og mellomstore bedrifter og andre foretak.

3. Kommisjonen skal utpeke medlemmene av det rådgivende forumet i samsvar med kriteriene fastsatt i nr. 2, blant interessenter med anerkjent sakkunnskap PÅ KI-OMRÅDET.

4. Mandatperioden for medlemmene av det rådgivende forumet skal være to år og kan forlenges med inntil fire år.

5. Byrået for grunnleggende rettigheter, ENISA, Den europeiske standardiseringskomité (CEN), Den europeiske komité for elektroteknisk standardisering (CENELEC) og Det europeiske standardiseringsinstituttet for telekommunikasjon (ETSI) skal være faste medlemmer av det rådgivende forumet.

6. Det rådgivende forumet skal utarbeide sin egen forretningsorden. Det skal velge to medformenn blant sine medlemmer, i samsvar med kriteriene fastsatt i nr. 2. Mandatperioden for de to formennene skal være to år og kan fornyes én gang.

7. Det rådgivende forumet skal avholde møter minst to ganger i året. Det rådgivende forumet kan invitere eksperter og andre interessenter til sine møter.

8. Det rådgivende forumet kan utarbeide uttalelser, anbefalinger og skriftlige bidrag på anmodning fra styret eller kommisjonen.

9. Det rådgivende forumet kan opprette permanente eller midlertidige undergrupper etter behov for å undersøke spesifikke spørsmål knyttet til målene i denne forordning.

10. Det rådgivende forumet skal utarbeide en årlig rapport om sin virksomhet. Rapporten skal gjøres offentlig tilgjengelig.

Artikkel 68

Vitenskapelig panel av uavhengige eksperter

1. Kommisjonen skal ved hjelp av en gjennomføringsrettsakt fastsette bestemmelser om opprettelse av et vitenskapelig panel av uavhengige eksperter ("det vitenskapelige panelet") som skal støtte håndhevingstiltakene i henhold til denne forordning. Denne gjennomføringsrettsakten skal vedtas i samsvar med framgangsmåten for behandling nevnt i artikkel 98 nr. 2.

2. Det vitenskapelige panelet skal bestå av eksperter som er utvalgt av Kommisjonen på grunnlag av oppdatert vitenskapelig eller teknisk sakkunnskap PÅ KI-området som er nødvendig for oppgavene fastsatt i nr. 3, og skal kunne godtgjøre at alle følgende vilkår er oppfylt

(a) har særlig ekspertise og kompetanse og vitenskapelig eller teknisk ekspertise innen AI;

(b) uavhengighet av leverandører av aI-systemer eller generelle aI-modeller;

(c) evne til å utføre aktiviteter med omhu, nøyaktighet og objektivitet.

Kommisjonen skal i samråd med styret fastsette antallet eksperter i panelet i samsvar med de nødvendige behovene, og skal sikre en rimelig kjønnsrepresentasjon og geografisk representasjon.

3. Det vitenskapelige panelet skal gi råd og støtte til aI-kontoret, særlig med hensyn til følgende oppgaver:

(a) støtte gjennomføringen og håndhevingen AV denne forordning når det gjelder generelle aI-modeller og -systemer, særlig ved å

(i) varsling av aI-kontoret om mulige systemiske risikoer på unionsnivå for generelle aI-modeller, i samsvar med artikkel 90;

(ii) bidra til utviklingen av verktøy og metoder for å evaluere egenskapene til generelle AI-modeller og -systemer, blant annet ved hjelp av benchmarks;

(iii) gi råd om klassifisering av generelle KI-modeller med systemrisiko;

(iv) gi råd om klassifisering av ulike generelle AI-modeller og -systemer;

(v) bidra til utviklingen av verktøy og maler;

(b) støtte arbeidet til markedsovervåkningsmyndighetene, på deres anmodning;

(c) støtte grenseoverskridende markedsovervåkingsaktiviteter som nevnt i artikkel 74 nr. 11, uten at det berører markedsovervåkingsmyndighetenes myndighet;

(d) støtte aI-kontoret i utførelsen av sine oppgaver I forbindelse med Unionens beskyttelsesprosedyre I henhold til artikkel 81.

4. Ekspertene i det vitenskapelige panelet skal utføre sine oppgaver upartisk og objektivt, og skal sikre konfidensialiteten til informasjon og data som innhentes under utførelsen av deres oppgaver og virksomhet. De skal verken be om eller motta instrukser fra noen når de utfører sine oppgaver i henhold til nr. 3. Hver ekspert skal utarbeide en interesseerklæring, som skal gjøres offentlig tilgjengelig. AI-kontoret skal etablere systemer og prosedyrer for aktivt å håndtere og forebygge potensielle interessekonflikter.

5. Gjennomføringsrettsakten nevnt i nr. 1 skal inneholde bestemmelser om vilkår, framgangsmåter og nærmere ordninger for vitenskapspanelet og dets medlemmer med hensyn til å utstede varsler og anmode om bistand fra AI-kontoret for utførelsen av vitenskapspanelets oppgaver.

Artikkel 69

Tilgang til ekspertpoolen for medlemsstatene

1. Medlemsstatene kan benytte seg av eksperter fra det vitenskapelige panelet for å støtte sine håndhevingsaktiviteter i henhold til denne forordning.

2. Medlemsstatene kan pålegges å betale gebyrer for råd og støtte fra ekspertene. Strukturen og nivået på gebyrene samt omfanget av og strukturen på de kostnader som kan kreves dekket, skal fastsettes i gjennomføringsrettsakten nevnt i artikkel 68 nr. 1, idet det tas hensyn til målene om en hensiktsmessig gjennomføring av denne forordning, kostnadseffektivitet og nødvendigheten av å sikre effektiv tilgang til eksperter for alle medlemsstatene.

3. Kommisjonen skal legge til rette for at medlemsstatene ved behov får tilgang til ekspertene i rett tid, og sikre at kombinasjonen av støtteaktiviteter som utføres av Unionens INTERNE utprøvingsstøtte I HENHOLD TIL artikkel 84 og eksperter i henhold til denne artikkel, er effektivt organisert og gir best mulig merverdi.

AVSNITT 2

Nasjonale kompetente myndigheter

Artikkel 70

Utpeking av nasjonale kompetente myndigheter og felles kontaktpunkter

1. Hver medlemsstat skal opprette eller utpeke minst én notifiserende myndighet og minst én markedstilsynsmyndighet som nasjonale vedkommende myndigheter for denne forordnings formål. Disse nasjonale vedkommende myndigheter skal utøve sine fullmakter uavhengig, upartisk og upartisk for å sikre objektiviteten i sin virksomhet og sine oppgaver og for å sikre anvendelsen og gjennomføringen av denne forordning. Medlemmene av disse myndighetene skal avstå fra enhver handling som er uforenlig med deres plikter. Forutsatt at disse prinsippene overholdes, kan slike aktiviteter og oppgaver utføres av en eller flere utpekte myndigheter, i samsvar med medlemsstatens organisatoriske behov.

2. Medlemsstatene skal underrette Kommisjonen om identiteten til meldermyndighetene og markedstilsynsmyndighetene og om disse myndighetenes oppgaver, samt om eventuelle senere endringer i disse. Medlemsstatene skal offentliggjøre informasjon om hvordan vedkommende myndigheter og kontaktpunktene kan kontaktes, ved hjelp av elektroniske kommunikasjonsmidler innen 2. august 2025. Medlemsstatene skal utpeke en markedstilsynsmyndighet som skal fungere som det felles kontaktpunktet for denne forordning, og skal underrette Kommisjonen om det felles kontaktpunktets identitet. Kommisjonen skal offentliggjøre en liste over de felles kontaktpunktene.

3. Medlemsstatene skal sikre at deres nasjonale vedkommende myndigheter har tilstrekkelige tekniske, økonomiske og menneskelige ressurser infrastruktur til å utføre sine oppgaver i henhold til denne forordning på en effektiv måte. De nasjonale vedkommende myndigheter skal særlig ha et tilstrekkelig antall ansatte som ER permanent tilgjengelige, og hvis kompetanse og sakkunnskap skal omfatte en inngående forståelse AV KI-teknologi, data og databehandling, vern av personopplysninger, nettsikkerhet, grunnleggende rettigheter, helse- og sikkerhetsrisikoer og kunnskap om eksisterende standarder og rettslige krav. Medlemsstatene skal vurdere og om nødvendig oppdatere kompetanse- og ressurskravene nevnt i dette ledd årlig basis.

4. Nasjonale vedkommende myndigheter skal treffe egnede tiltak for å sikre et tilstrekkelig cybersikkerhetsnivå.

5. Når de nasjonale vedkommende myndigheter utfører sine oppgaver, skal de handle i samsvar med taushetsplikten fastsatt i artikkel 78.

6. Innen 2. august 2025, og deretter hvert annet år, skal medlemsstatene rapportere til Kommisjonen om status for de nasjonale vedkommende myndigheters finansielle og menneskelige ressurser, med en vurdering av om de er tilstrekkelige. Kommisjonen skal oversende denne informasjonen til styret for drøfting og eventuelle anbefalinger.

7. Kommisjonen skal legge til rette for utveksling av erfaringer mellom nasjonale vedkommende myndigheter.

8. Nasjonale vedkommende myndigheter kan gi veiledning og råd om gjennomføringen av denne forordning, særlig til små og mellomstore bedrifter, herunder nyetablerte foretak, idet det tas hensyn til veiledningen og rådene fra styret og Kommisjonen, alt etter hva som er relevant. Når nasjonale vedkommende myndigheter HAR hensikt å gi veiledning og råd med hensyn til et AI-system på områder som omfattes av annen unionsrett, skal de nasjonale vedkommende myndigheter i henhold til denne unionsretten konsulteres, alt etter hva som er hensiktsmessig.

9. Når Unionens institusjoner, organer, kontorer eller byråer omfattes av denne forordning, skal Den europeiske datatilsynsmann fungere som vedkommende myndighet for tilsynet med dem.

CHaPTER VIII

EU-DATABASE FOR HØYRISIKO AI-SYSTEMER

Artikkel 71

EU-database for høyrisikosystemer for kunstig intelligens oppført i vedlegg III

1. Kommisjonen skal i samarbeid med medlemsstatene opprette og vedlikeholde en EU-database med opplysninger nevnt i nr. 2 og 3 i denne artikkel om høyrisikosystemer for KUNSTIG INTELLIGENS nevnt i artikkel 6 nr. 2, som er registrert i samsvar med artikkel 49 og 60, og systemer for KUNSTIG INTELLIGENS som ikke anses som høyrisikosystemer I henhold til artikkel 6 nr. 3, og som er registrert i samsvar med artikkel 6 nr. 4 og artikkel 49. Ved fastsettelse av de funksjonelle spesifikasjonene for en slik database skal Kommisjonen rådføre seg med de relevante ekspertene, og ved oppdatering av de funksjonelle spesifikasjonene for en slik database skal Kommisjonen rådføre seg med Personvernrådet.

2. Opplysningene som er oppført i avsnitt A og B i vedlegg VIII, skal legges inn i EU-databasen av leverandøren eller, der det er relevant, av den autoriserte representanten.

3. Opplysningene som er oppført i avsnitt C i vedlegg VIII, skal legges inn i EU-databasen av utplassøren som er, eller som opptrer på vegne av, en offentlig myndighet, et byrå eller et organ, i samsvar med artikkel 49 nr. 3 og 4.

4. Med unntak av den delen som er nevnt i artikkel 49 nr. 4 og artikkel 60 nr. 4 bokstav c), skal opplysningene i EU-databasen som er registrert i samsvar med artikkel 49, være tilgjengelige og offentlig tilgjengelige på en brukervennlig måte. Informasjonen skal være lett å navigere i og maskinlesbar. Opplysningene som er registrert i samsvar med artikkel 60, skal bare være tilgjengelige for markedstilsynsmyndighetene og Kommisjonen, med mindre den potensielle leverandøren eller leverandøren har gitt samtykke til at opplysningene også gjøres tilgjengelige for allmennheten.

5. EU-databasen skal inneholde personopplysninger bare i den grad det er nødvendig for å samle inn og behandle opplysninger i samsvar med denne forordning. Disse opplysningene skal omfatte navn og kontaktopplysninger for fysiske personer som er ansvarlige for registreringen av systemet, og som har rettslig myndighet til å representere leverandøren eller utbyggeren, alt etter hva som er relevant.

6. Kommisjonen skal være behandlingsansvarlig for EU-databasen. Den skal gi tilbydere, potensielle tilbydere og distributører tilstrekkelig teknisk og administrativ støtte. EU-databasen skal oppfylle gjeldende krav til tilgjengelighet.

CHaPTER IX

OVERVÅKING ETTER MARKEDSFØRING, INFORMASJONSDELING OG MARKEDSOVERVÅKING

AVSNITT 1

Overvåking etter markedsføring

Artikkel 72

Overvåking etter markedsføring av leverandører og plan for overvåking etter markedsføring av AI-systemer med høy risiko

1. Leverandørene skal etablere og dokumentere et system for overvåking etter at utstyret er brakt i omsetning, på en måte som står I forhold til aI-teknologienes art og risikoen ved høyrisiko aI-systemet.

2. Systemet for overvåking etter at utstyret er brakt i omsetning, skal aktivt og systematisk samle inn, dokumentere og analysere relevante data som kan framskaffes av driftsansvarlige eller som kan samles inn gjennom andre kilder, om ytelsen til høyrisiko-AI-systemer gjennom hele deres levetid, og som gjør det mulig for leverandøren å evaluere aI-systemers kontinuerlige samsvar med kravene fastsatt i kapittel III, avsnitt 2. Der det er relevant, skal overvåking etter at utstyret er brakt I omsetning, omfatte en analyse av samspillet med andre . Denne plikten skal ikke omfatte sensitive driftsdata fra utplasserere som er rettshåndhevende myndigheter.

3. Systemet for overvåking etter at utstyret er brakt i omsetning, skal være basert på en plan for overvåking etter at utstyret er brakt i omsetning. Planen for overvåking etter at utstyret er brakt i omsetning, skal være en del av den tekniske dokumentasjonen nevnt i vedlegg IV. Kommisjonen skal vedta en gjennomføringsrettsakt med nærmere bestemmelser om fastsettelse av en mal for planen for overvåking etter at utstyret er brakt i omsetning, og en liste over elementer som skal inngå i planen, innen 2. februar 2026. Denne gjennomføringsrettsakten skal vedtas i samsvar med framgangsmåten for behandling nevnt i artikkel 98 nr. 2.

4. For høyrisiko-AI-systemer som omfattes av Unionens harmoniseringslovgivning oppført i avsnitt A i vedlegg I, der det allerede er etablert et system og en plan for overvåking etter at utstyret er brakt i omsetning i henhold til nevnte lovgivning, skal leverandørene, for å sikre konsekvens, unngå dobbeltarbeid og minimere tilleggsbyrder, kunne velge å integrere de nødvendige elementene beskrevet i nr. 1, 2 og 3 ved hjelp av malen nevnt i nr. 3 i systemer og planer som allerede finnes i henhold til nevnte lovgivning, forutsatt at de oppnår et tilsvarende beskyttelsesnivå, alt etter hva som er hensiktsmessig.

Første ledd i dette nummer får også anvendelse på høyrisikosystemer som nevnt i nr. 5 i vedlegg III, som er markedsført eller tatt i bruk av finansinstitusjoner som er underlagt krav i henhold til unionsretten om finansielle tjenester med hensyn til deres interne styring, ordninger eller prosesser.

AVSNITT 2

Deling av informasjon om alvorlige hendelser

Artikkel 73

Rapportering av alvorlige hendelser

1. Leverandører AV høyrisiko-AI-systemer som markedsføres på unionsmarkedet, skal rapportere enhver alvorlig hendelse til markedstilsynsmyndighetene i de medlemsstatene der hendelsen inntraff.

2. Rapporten nevnt i nr. 1 skal avgis umiddelbart etter at leverandøren har fastslått en årsakssammenheng mellom KI-systemet og den alvorlige hendelsen eller en rimelig sannsynlighet for en slik , og under alle omstendigheter senest 15 dager etter at leverandøren eller, der det er relevant, utplasseringsselskapet, får kjennskap til den alvorlige hendelsen.

Fristen for rapportering nevnt i første ledd skal ta hensyn til alvorlighetsgraden av den alvorlige hendelsen.

3. Uten hensyn til nr. 2 i denne artikkel skal rapporten nevnt i nr. 1 i denne artikkel, i tilfelle av en omfattende overtredelse eller en alvorlig hendelse som definert i artikkel 3 nr. 49 bokstav b), leveres umiddelbart og senest to dager etter at leverandøren eller, der det er relevant, utplassøren blir kjent med hendelsen.

4. Uten hensyn til nr. 2 skal rapporten, dersom en person dør, avgis umiddelbart etter at leverandøren eller utplassøren har fastslått, eller så snart det foreligger mistanke om, en årsakssammenheng mellom høyrisiko-AI-systemet og den alvorlige hendelsen, men ikke senere enn ti dager etter at leverandøren eller, der det er relevant, utplassøren får kjennskap til den alvorlige hendelsen.

5. Dersom det er nødvendig for å sikre rettidig rapportering, kan leverandøren eller, der det er aktuelt, utplasseringsselskapet, sende inn en første rapport som er ufullstendig, etterfulgt av en fullstendig rapport.

6. Etter at en alvorlig hendelse er rapportert I henhold til nr. 1, skal leverandøren uten opphold foreta de nødvendige undersøkelser av den alvorlige hendelsen og det berørte AI-systemet. Dette skal omfatte en risikovurdering av hendelsen og korrigerende tiltak.

Leverandøren skal samarbeide med vedkommende myndigheter og, dersom det er relevant, med det berørte meldte organet under undersøkelsene nevnt I første ledd, og skal ikke foreta undersøkelser som innebærer at det berørte AI-systemet endres på en måte som kan påvirke en eventuell senere vurdering av årsakene til hendelsen, før vedkommende myndigheter er underrettet om dette.

7. Ved mottak av melding om en alvorlig hendelse som nevnt i artikkel 3 nr. 49 bokstav c), skal den relevante markedstilsynsmyndigheten underrette de nasjonale offentlige myndigheter eller organer nevnt i artikkel 77 nr. 1. Kommisjonen skal utarbeide en særskilt veiledning for å gjøre det lettere å oppfylle forpliktelsene fastsatt i nr. 1 i denne artikkel. Denne veiledningen skal utstedes innen 2. august 2025 og skal vurderes regelmessig.

8. Markedstilsynsmyndigheten skal treffe egnede tiltak, fastsatt i artikkel 19 i forordning (EU) 2019/1020, innen sju dager fra den datoen den mottok meldingen nevnt i nr. 1 i denne artikkel, og skal følge meldingsprosedyrene som fastsatt i nevnte forordning.

9. For høyrisiko-AI-systemer nevnt i vedlegg III som er brakt I omsetning eller tatt i bruk av leverandører som er underlagt unionsrettsakter som fastsetter rapporteringskrav tilsvarende dem som er fastsatt i denne forordning, skal melding om alvorlige hendelser begrenses til dem som er nevnt i artikkel 3 nr. 49 bokstav c).

10. For høyrisiko-AI-systemer som er sikkerhetskomponenter i utstyr, eller som i seg selv er utstyr som omfattes av forordning (EU) 2017/745 og (EU) 2017/746, skal melding om alvorlige hendelser begrenses til dem som er nevnt i artikkel 3 nr. 49 bokstav c) i denne forordning, og skal sendes til den nasjonale vedkommende myndighet som er valgt for dette formål av medlemsstaten der hendelsen inntraff.

11. Nasjonale vedkommende myndigheter skal umiddelbart underrette Kommisjonen om enhver alvorlig hendelse, uavhengig av om de har iverksatt tiltak eller ikke, i samsvar med artikkel 20 i forordning (EU) 2019/1020.

AVSNITT 3

Håndhevelse

Artikkel 74

Markedsovervåking og kontroll av AI-systemer i EU-markedet

1. Forordning (EU) 2019/1020 skal få anvendelse på AI-systemer som omfattes av denne forordning. Med henblikk på effektiv håndheving av denne forordning:

(a) skal enhver henvisning til en økonomisk aktør i henhold til forordning (EU) 2019/1020 forstås som å omfatte alle aktører som er angitt i artikkel 2 nr. 1 i denne forordning;

(b) enhver henvisning til et produkt i henhold til forordning (EU) 2019/1020 skal forstås som å omfatte alle AI-systemer som faller inn under denne forordningens virkeområde.

2. Som en del av sine rapporteringsforpliktelser i henhold til artikkel 34 nr. 4 i forordning (EU) 2019/1020 skal markedstilsynsmyndighetene årlig rapportere til Kommisjonen og relevante nasjonale konkurransemyndigheter om all informasjon som er identifisert i løpet av markedstilsynsvirksomheten, og som kan være av potensiell interesse for anvendelsen av unionsretten om konkurranseregler. De skal også årlig rapportere til Kommisjonen om bruk av forbudt praksis som har forekommet i løpet av det året, og om hvilke tiltak som er truffet.

3. For høyrisiko-AI-systemer knyttet til produkter som omfattes av Unionens harmoniseringsregelverk oppført i avsnitt A i vedlegg I, skal markedstilsynsmyndigheten I henhold til denne forordning være den myndighet som er ansvarlig for markedstilsynsaktiviteter utpekt i henhold til disse rettsaktene.

Som unntak fra første ledd kan medlemsstatene under egnede omstendigheter utpeke en annen relevant myndighet til å fungere som markedstilsynsmyndighet, forutsatt at de sikrer samordning med de relevante sektorielle markedstilsynsmyndighetene med ansvar for håndheving av Unionens harmoniseringsregelverk oppført i vedlegg I.

4. Framgangsmåtene nevnt i artikkel 79-83 i denne forordning får ikke anvendelse på AI-systemer knyttet til produkter som omfattes av Unionens harmoniseringsregelverk oppført i avsnitt A i vedlegg I, dersom slike rettsakter allerede fastsetter framgangsmåter som sikrer et tilsvarende beskyttelsesnivå og har samme formål. I slike tilfeller skal de relevante sektorprosedyrene få anvendelse i stedet.

5. Uten at det berører markedstilsynsmyndighetenes myndighet i henhold til artikkel 14 i forordning (EU) 2019/1020, kan markedstilsynsmyndighetene for å sikre effektiv håndheving av denne forordning utøve myndigheten nevnt i artikkel 14 nr. 4 bokstav d) og j) i nevnte forordning eksternt, alt etter hva som er relevant.

6. For høyrisiko-AI-systemer som bringes i , tas i bruk eller brukes av finansinstitusjoner som regulert av unionsretten om finansielle tjenester, skal markedstilsynsmyndigheten i henhold til denne forordning være den relevante nasjonale myndighet som er ansvarlig for finanstilsyn med disse institusjonene i henhold til nevnte lovgivning, I DEN utstrekning markedsføringen, IBRUKTAKINGEN eller bruken AV AI-systemet er i direkte tilknytning til ytelsen AV disse finansielle tjenestene.

7. Som unntak fra nr. 6 kan medlemsstaten under egnede omstendigheter, og forutsatt at samordningen er sikret, utpeke en annen relevant myndighet som markedstilsynsmyndighet i henhold til denne forordning.

Nasjonale markedstilsynsmyndigheter som fører tilsyn med regulerte kredittinstitusjoner som er regulert i henhold til direktiv 2013/36/EU, og som deltar i den felles tilsynsmekanismen som er opprettet ved forordning (EU) nr. 1024/2013, bør uten opphold rapportere til Den europeiske sentralbanken all informasjon som er identifisert i løpet av deres markedstilsynsaktiviteter, og som kan være av potensiell interesse for Den europeiske sentralbankens tilsynsoppgaver som er spesifisert i nevnte forordning.

8. For HØYRISIKO-AI-SYSTEMER oppført i nr. 1 i vedlegg III til denne forordning, i den utstrekning systemene brukes til rettshåndhevelse, grenseforvaltning og rettsvesen og demokrati, og for høyrisiko-AI-systemer oppført i nr. 6, 7 og 8 i vedlegg III til denne forordning, skal medlemsstatene utpeke som markedstilsynsmyndigheter for denne forordnings formål enten de kompetente datatilsynsmyndigheter I henhold til forordning (EU) 2016/679 eller direktiv (EU) 2016/680, eller enhver annen myndighet som er utpekt i henhold til de samme vilkår som fastsatt i artikkel 41-44 i direktiv (EU) 2016/680. Markedsovervåkingsaktiviteter skal ikke på noen måte påvirke rettslige myndigheters uavhengighet eller på annen måte gripe inn i deres virksomhet når de opptrer i egenskap av rettslige myndigheter.

9. Når Unionens institusjoner, organer, kontorer eller byråer omfattes av denne forordning, skal Den europeiske datatilsynsmann opptre som deres markedstilsynsmyndighet, med unntak av Den europeiske unions domstol når den opptrer i egenskap av domstol.

10. Medlemsstatene skal legge til rette for samordning mellom markedstilsynsmyndigheter som er utpekt i henhold til denne forordning, og andre relevante nasjonale myndigheter eller organer som fører tilsyn anvendelsen av Unionens harmoniseringslovgivning oppført i vedlegg I eller I annen unionsrett, som kan være relevant FOR høyrisiko-AI-systemene nevnt I vedlegg III.

11. Markedstilsynsmyndighetene og Kommisjonen skal kunne foreslå felles aktiviteter, herunder felles undersøkelser, som skal gjennomføres av enten markedstilsynsmyndighetene eller markedstilsynsmyndighetene sammen med Kommisjonen, og som har som mål å fremme etterlevelse, identifisere manglende etterlevelse, øke bevisstheten eller gi veiledning i forbindelse med denne forordning med hensyn til bestemte kategorier av høyrisikosystemer FOR aI som er funnet å utgjøre en alvorlig risiko i to eller flere medlemsstater I samsvar med artikkel 9 I forordning (EU) 2019/1020. aI-kontoret skal gi koordineringsstøtte til felles etterforskninger.

12. Uten at det berører de fullmakter som er fastsatt I forordning (EU) 2019/1020, og der det er relevant og begrenset til det som er nødvendig for å utføre deres oppgaver, skal markedstilsynsmyndighetene gis full tilgang av tilbyderne til dokumentasjonen samt opplærings-, validerings- og testdatasettene som brukes til utvikling AV høyrisiko-AI-systemer, herunder, der det er relevant og med forbehold for sikkerhetstiltak, gjennom grensesnitt for applikasjonsprogrammering (API) eller andre relevante tekniske midler og verktøy som muliggjør ekstern tilgang.

13. Markedstilsynsmyndighetene skal gis tilgang til kildekoden TIL høyrisiko-AI-systemet etter begrunnet anmodning og bare når begge følgende vilkår er oppfylt:

(a) tilgang til kildekoden er nødvendig for å vurdere om et høyrisiko-AI-system er i samsvar med kravene fastsatt i kapittel III, avsnitt 2; og

(b) test- eller revisjonsprosedyrer og verifikasjoner basert på data og dokumentasjon fra leverandøren er uttømt eller har vist seg å være utilstrekkelige.

14. all informasjon eller dokumentasjon som innhentes av markedstilsynsmyndighetene, skal behandles i samsvar konfidensialitetsforpliktelsene fastsatt i artikkel 78.

Artikkel 75

Gjensidig assistanse, markedsovervåking og kontroll av generelle AI-systemer

1. Dersom et aI-system er basert på en generell aI-modell, og modellen og systemet er utviklet av samme leverandør, skal aI-kontoret ha myndighet til å overvåke og føre tilsyn med at AI-SYSTEMET oppfyller forpliktelsene i henhold til denne forordning. For å utføre sine overvåkings- og tilsynsoppgaver skal aI-kontoret ha alle de fullmakter en markedstilsynsmyndighet har i henhold til dette avsnitt og forordning (EU) 2019/1020.

2. Dersom de relevante markedstilsynsmyndighetene har tilstrekkelig grunn til å anse at allmenne aI-systemer som kan brukes direkte av utplasserere til minst ett formål som er klassifisert som høyrisiko i henhold til denne forordning, ikke er i samsvar med kravene fastsatt i denne forordning, skal de samarbeide med aI-kontoret for å gjennomføre samsvarsvurderinger, og skal informere styret og andre markedstilsynsmyndigheter om dette.

3. Dersom en markedstilsynsmyndighet ikke er i stand til å fullføre undersøkelse av høyrisiko-ali-systemet på grunn av manglende tilgang til visse opplysninger knyttet til den generelle aI-modellen, til tross for at den har gjort alle egnede anstrengelser for å innhente disse opplysningene, kan den inngi begrunnet anmodning til aI-kontoret, som skal håndheve tilgangen til disse opplysningene. I så fall skal aI-kontoret uten opphold, og under alle omstendigheter innen 30 dager, gi søkermyndigheten all informasjon som aI-kontoret anser som relevant for å fastslå om et høyrisiko-aiI-system ikke er i samsvar med kravene. Markedstilsynsmyndighetene skal sikre konfidensialiteten til informasjonen de innhenter i samsvar med artikkel 78 i denne forordning. Fremgangsmåten fastsatt i kapittel VI i forordning (EU) 2019/1020 får *tilsvarende* anvendelse.

Artikkel 76

Markedsovervåkningsmyndighetene fører tilsyn med testing under reelle forhold

1. Markedstilsynsmyndighetene skal ha kompetanse og myndighet til å sikre at testing under reelle forhold er i samsvar med denne forordning.

2. Når testing under reelle forhold utføres for KI-systemer som er underlagt tilsyn i en sandkasse for KI-regulering i henhold til artikkel 58, skal markedstilsynsmyndighetene kontrollere at artikkel 60 overholdes som en del av deres tilsynsrolle for sandkassen for KI-regulering. Disse myndighetene kan, dersom det er hensiktsmessig, tillate at testingen under reelle forhold utføres av leverandøren eller den potensielle leverandøren, som unntak fra vilkårene fastsatt i artikkel 60 nr. 4 bokstav f) og g).

3. Dersom en markedstilsynsmyndighet har blitt informert av den potensielle tilbyderen, tilbyderen eller en om en alvorlig hendelse eller har andre grunner til å mene at vilkårene fastsatt i artikkel 60 og 61 ikke er oppfylt, kan den treffe en av følgende beslutninger på sitt territorium, alt etter hva som er hensiktsmessig

(a) for å avbryte eller avslutte testingen under reelle forhold;

(b) å kreve at leverandøren eller den potensielle leverandøren og utrulleren eller den potensielle utrulleren modifiserer ethvert aspekt av testingen under virkelige forhold.

4. Dersom en markedstilsynsmyndighet har truffet beslutning som nevnt i nr. 3 i denne artikkel, eller har gjort innsigelse i henhold til artikkel 60 nr. 4 bokstav b), skal beslutningen eller innsigelsen angi begrunnelsen for den og hvordan tilbyderen eller den potensielle tilbyderen kan påklage beslutningen eller innsigelsen.

5. Dersom det er relevant, skal en markedstilsynsmyndighet som har truffet en beslutning som nevnt i nr. 3, underrette markedstilsynsmyndighetene i de andre medlemsstatene der KI-systemet er blitt testet i samsvar med testplanen, om begrunnelsen for beslutningen.

Artikkel 77

Beføyelser til myndigheter som beskytter grunnleggende rettigheter

1. Nasjonale offentlige myndigheter eller organer som fører tilsyn med eller håndhever overholdelsen av forpliktelser i henhold til unionsretten som beskytter grunnleggende rettigheter, herunder retten til ikke-diskriminering, i forbindelse med bruken av høyrisikosystemer som nevnt i vedlegg III, skal ha myndighet til å anmode om og få tilgang til all dokumentasjon som er utarbeidet eller oppbevares i henhold til denne forordning, på et tilgjengelig språk og I et tilgjengelig format når tilgang til denne dokumentasjonen er nødvendig for at de effektivt skal kunne oppfylle sine mandater innenfor rammen av sin jurisdiksjon. Den relevante offentlige myndigheten eller det relevante offentlige organet skal underrette markedstilsynsmyndigheten i den berørte medlemsstaten om enhver slik anmodning.

2. Senest 2. november 2024 skal hver medlemsstat identifisere de offentlige myndighetene eller organene nevnt i nr. 1 gjøre en liste over dem offentlig tilgjengelig. Medlemsstatene skal underrette Kommisjonen og de andre medlemsstatene om listen, og skal holde listen oppdatert.

3. Dersom dokumentasjonen nevnt i nr. 1 ikke er tilstrekkelig til å fastslå om det har forekommet en overtredelse av forpliktelsene i henhold til unionsretten om beskyttelse av grunnleggende rettigheter, kan den offentlige myndigheten eller det offentlige organet nevnt I NR. 1 rette en begrunnet anmodning til markedstilsynsmyndigheten om å organisere testing av høyrisikosystemet ved hjelp av tekniske midler. Markedstilsynsmyndigheten skal organisere testingen i nært samarbeid med den offentlige myndigheten eller det offentlige organet som har fremsatt anmodningen, innen rimelig tid etter at anmodningen er fremsatt.

4. skal all informasjon eller dokumentasjon som de nasjonale offentlige myndigheter eller organer nevnt i nr. 1 denne artikkel innhenter i henhold til denne artikkel, behandles i samsvar med taushetsplikten fastsatt i artikkel 78.

Artikkel 78

Konfidensialitet

1. Kommisjonen, markedstilsynsmyndighetene og meldte organer og enhver annen fysisk eller juridisk person som er involvert i anvendelsen av denne forordning, skal i samsvar med unionsretten eller nasjonal rett respektere konfidensialiteten til informasjon og som innhentes i forbindelse med utførelsen av deres oppgaver og virksomhet, på en slik måte at det særlig sikres beskyttelse av

(a) immaterielle rettigheter og konfidensiell forretningsinformasjon eller forretningshemmeligheter tilhørende en fysisk eller juridisk person, herunder kildekode, unntatt i de tilfeller som er nevnt i artikkel 5 i Europaparlamentets og Rådets direktiv (EU) 2016/943 ([57])

(b) effektiv gjennomføring av denne forordning, særlig i forbindelse med inspeksjoner, undersøkelser eller revisjoner;

(c) offentlige og nasjonale sikkerhetsinteresser;

(d) gjennomføringen av straffe- eller forvaltningssaker;

(e) informasjon som er gradert i henhold til unionsretten eller nasjonal rett.

2. Myndighetene som deltar i anvendelsen av denne forordning i henhold til nr. 1, skal bare anmode om opplysninger som ER strengt nødvendige for å vurdere risikoen VED KI-systemer og for å utøve sine fullmakter I samsvar med denne forordning og forordning (EU) 2019/1020. De skal innføre tilstrekkelige og effektive cybersikkerhetstiltak for å beskytte sikkerheten og konfidensialiteten til informasjonen og opplysningene som innhentes, og skal slette de innhentede opplysningene så snart de ikke lenger er nødvendige for det formålet de ble innhentet for, i samsvar med gjeldende unionsrett eller nasjonal rett.

3. Uten at det berører nr. 1 og 2, skal opplysninger som utveksles konfidensielt mellom nasjonale vedkommende myndigheter eller mellom nasjonale vedkommende myndigheter og Kommisjonen, ikke utleveres uten forutgående samråd med den opprinnelige nasjonale vedkommende myndighet og utrulleren når høyrisiko-AI-systemer nevnt i nr. 1, 6 eller 7 i vedlegg III brukes av rettshåndhevelses-, grensekontroll-, innvandrings- eller asylmyndigheter, og når slik utlevering ville sette offentlige og nasjonale sikkerhetsinteresser i fare. Denne informasjonsutvekslingen skal ikke omfatte sensitive operative data i forbindelse med , grensekontroll-, innvandrings- eller asylmyndighetenes virksomhet.

Når rettshåndhevelses-, innvandrings- eller asylmyndighetene er leverandører av høyrisikosystemer som nevnt i nr. 1, 6 eller 7 i vedlegg III, skal den tekniske dokumentasjonen nevnt i vedlegg IV forbli i disse myndighetenes lokaler. Disse myndighetene skal sikre at markedstilsynsmyndighetene nevnt i artikkel 74 nr. 8 og 9, alt etter hva som er relevant, på anmodning umiddelbart kan få tilgang til dokumentasjonen eller få en kopi av den. Bare ansatte hos markedstilsynsmyndigheten som innehar sikkerhetsklarering på riktig nivå, skal ha tilgang til denne dokumentasjonen eller en kopi av den.

4. Nr. 1, 2 og 3 skal ikke berøre Kommisjonens, medlemsstatenes og deres relevante myndigheters rettigheter eller forpliktelser, eller de meldte organers rettigheter eller forpliktelser med hensyn til utveksling av opplysninger og formidling av advarsler, herunder i forbindelse med samarbeid over landegrensene, og de skal heller ikke berøre de berørte parters forpliktelser til å gi opplysninger i henhold til medlemsstatenes straffelovgivning.

5. Kommisjonen og medlemsstatene kan om nødvendig og i samsvar med relevante bestemmelser i internasjonale avtaler og handelsavtaler utveksle fortrolige opplysninger med reguleringsmyndigheter i tredjestater som de har inngått bilaterale eller multilaterale avtaler om konfidensialitet med, og som garanterer et tilstrekkelig konfidensialitetsnivå.

Artikkel 79

Prosedyre på nasjonalt nivå for håndtering av AI-systemer som utgjør en risiko

1. aI-systemer som utgjør en risiko, skal forstås som et "produkt som utgjør en risiko" som definert i artikkel 3 nr. 19 i forordning (EU) 2019/1020, I DEN grad de utgjør en risiko for menneskers helse eller sikkerhet eller grunnleggende rettigheter.

2. Dersom markedstilsynsmyndigheten I en medlemsstat har tilstrekkelig grunn til å anse at et KI-system utgjør en risiko som nevnt i nr. 1 i denne artikkel, skal den foreta en evaluering av det berørte KI-systemet med hensyn til om det er I samsvar med alle krav og forpliktelser fastsatt i denne forordning. Det skal rettes særlig oppmerksomhet mot KI-systemer som utgjør en risiko for sårbare grupper. Dersom det identifiseres risikoer for grunnleggende rettigheter, skal markedstilsynsmyndigheten også informere og samarbeide fullt ut med de relevante nasjonale offentlige myndigheter eller organer nevnt i artikkel
77(1). De relevante markedsdeltakerne skal om nødvendig samarbeide med markedstilsynsmyndigheten og med de andre nasjonale offentlige myndighetene eller organene nevnt i artikkel 77 nr. 1.

(57) Europaparlaments- og rådsdirektiv (EU) 2016/943 av 8. juni 2016 om vern av ikke offentliggjort knowhow og forretningsinformasjon (forretningshemmeligheter) mot ulovlig tilegnelse, bruk og utlevering (EUT L 157 av 15.6.2016, s. 1).

Dersom markedstilsynsmyndigheten eller, dersom det er relevant, markedstilsynsmyndigheten i samarbeid med den nasjonale offentlige myndigheten nevnt i artikkel 77 nr. 1, i løpet av denne evalueringen finner at AI-SYSTEMET ikke oppfyller kravene og forpliktelsene fastsatt i denne forordning, skal den uten unødig opphold kreve at den relevante driftsansvarlige treffer alle egnede korrigerende tiltak for å bringe AI-SYSTEMET I samsvar med kravene og forpliktelsene fastsatt I denne forordning, skal den uten unødig opphold kreve at den relevante driftsansvarlige treffer alle egnede korrigerende tiltak for å bringe aI-systemet I samsvar med kravene, trekke aI-systemet tilbake fra markedet eller tilbakekalle det innen en frist som markedstilsynsmyndigheten kan fastsette, og under alle omstendigheter innen 15 virkedager, eller, dersom dette er kortere, i henhold til den relevante harmoniseringslovgivningen i Unionen.

Markedstilsynsmyndigheten skal underrette det relevante meldte organet om dette. artikkel 18 i forordning (EU) 2019/1020 får anvendelse på tiltakene nevnt i annet ledd i dette nummer.

3. Dersom markedstilsynsmyndigheten mener at den manglende etterlevelsen ikke er begrenset til dens nasjonale territorium, skal den uten ugrunnet opphold underrette Kommisjonen og de øvrige medlemsstatene om resultatene av evalueringen og om de tiltak den har pålagt den driftsansvarlige å treffe.

4. Den driftsansvarlige skal sikre at alle hensiktsmessige korrigerende tiltak treffes med hensyn til alle de berørte AI-systemene som den driftsansvarlige har gjort tilgjengelig på unionsmarkedet.

5. Dersom den driftsansvarlige for et KI-system ikke treffer egnede korrigerende tiltak innen fristen nevnt i nr. 2, skal markedstilsynsmyndigheten treffe alle egnede midlertidige tiltak for å forby eller begrense tilgjengeliggjøringen av KI-systemet på sitt nasjonale marked eller ibruktakingen av det, for å trekke produktet eller det frittstående KI-systemet tilbake fra markedet eller for å tilbakekalle det. Denne myndigheten skal uten ugrunnet opphold underrette Kommisjonen og de andre medlemsstatene om disse tiltakene.

6. Meldingen nevnt I nr. 5 skal inneholde alle tilgjengelige opplysninger, særlig den informasjonen som er nødvendig for å identifisere det AI-SYSTEMET som ikke oppfyller KRAVENE, aI-SYSTEMETS og forsyningskjedens opprinnelse, arten av den påståtte manglende oppfyllelsen av kravene og den involverte risikoen, arten og varigheten av de nasjonale tiltakene som er truffet, og de argumentene som den relevante aktøren har lagt fram. Markedstilsynsmyndighetene skal særlig angi om den manglende overholdelsen skyldes ett eller flere av følgende forhold

(a) manglende overholdelse av forbudet mot de ULOVLIGE handlingene SOM er nevnt i artikkel 5;

(b) ET høyrisiko-AI-system som ikke oppfyller kravene i kapittel III, avsnitt 2;

(c) mangler i de harmoniserte standardene eller felles spesifikasjonene nevnt i artikkel 40 og 41, som gir en presumsjon om samsvar;

(d) manglende overholdelse av artikkel 50.

7. Andre markedstilsynsmyndigheter enn markedstilsynsmyndigheten i den medlemsstaten som innleder framgangsmåten, skal uten unødig opphold underrette Kommisjonen og de andre medlemsstatene om eventuelle tiltak som ER truffet, og om eventuelle tilleggsopplysninger de HAR til rådighet om det berørte AI-systemets manglende samsvar, og, dersom de er uenige i det varslede nasjonale tiltaket, om sine innvendinger.

8. Dersom verken en markedstilsynsmyndighet i en medlemsstat eller Kommisjonen innen tre måneder etter av meldingen nevnt i . 5 i denne artikkel har reist innvendinger mot et midlertidig tiltak truffet av en markedstilsynsmyndighet i en annen medlemsstat, skal dette tiltaket anses som berettiget. Dette skal ikke berøre den berørte driftsansvarliges prosessuelle rettigheter i samsvar med artikkel 18 i forordning (EU) 2019/1020. Tremånedersperioden nevnt i dette ledd skal reduseres til 30 dager forbudet mot DEN ULOVLIGE praksisen nevnt I artikkel 5 I denne forordning ikke overholdes.

9. Markedstilsynsmyndighetene skal sørge for at det treffes egnede restriktive tiltak med hensyn til det berørte produktet eller AI-systemet, f.eks. tilbaketrekking av produktet ELLER AI-systemet fra deres marked, uten unødig opphold.

Artikkel 80

Prosedyre for håndtering av AI-systemer som leverandøren har klassifisert som ikke-høy risiko i henhold til vedlegg III

1. Dersom en markedstilsynsmyndighet har tilstrekkelig grunn til å anta at et aI-system som tilbyderen har klassifisert som et system uten høy risiko i henhold til artikkel 6 nr. 3, faktisk er et høyrisikosystem, skal markedstilsynsmyndigheten foreta en vurdering det aktuelle AI-SYSTEMET med hensyn til klassifiseringen som et høyrisikosystem på grunnlag av vilkårene fastsatt i artikkel 6 nr. 3 og Kommisjonens retningslinjer.

2. Dersom markedstilsynsmyndigheten i løpet av denne evalueringen finner at det berørte aI-systemet utgjør en høy risiko, skal den uten ugrunnet opphold kreve at den aktuelle leverandøren treffer alle nødvendige tiltak for å bringe aI-systemet I samsvar med kravene og forpliktelsene fastsatt i denne forordning, samt treffe egnede korrigerende tiltak innen en frist som markedstilsynsmyndigheten kan fastsette.

3. Dersom markedstilsynsmyndigheten anser at bruken av det berørte AI-systemet ikke er begrenset til dens nasjonale territorium, skal den uten unødig opphold underrette Kommisjonen og de andre medlemsstatene om resultatene av evalueringen og om de tiltak den har pålagt leverandøren å treffe.

4. Tilbyderen skal sikre at alle nødvendige tiltak treffes for å bringe AI-SYSTEMET i samsvar med kravene og forpliktelsene fastsatt i denne forordning. Dersom leverandøren av et berørt aI-system ikke bringer aI-systemet I samsvar med disse kravene og forpliktelsene innen fristen nevnt i nr. 2 i denne artikkel, skal leverandøren ilegges bøter i samsvar med artikkel 99.

5. Tilbyderen skal sikre at alle egnede korrigerende tiltak treffes med hensyn til alle de berørte AI-systemene som han har gjort tilgjengelig på unionsmarkedet.

6. Dersom leverandøren av det berørte AI-systemet ikke treffer tilstrekkelige korrigerende tiltak innen fristen i nr. 2 i denne artikkel, får artikkel 79 nr. 5 til 9 anvendelse.

7. Dersom markedstilsynsmyndigheten i løpet av evalueringen i henhold til nr. 1 i denne artikkel fastslår AT KI-systemet ble feilklassifisert av tilbyderen som ikke-høyrisiko for å omgå av kravene i kapittel III, avsnitt 2, skal tilbyderen ilegges bøter i samsvar med artikkel 99.

8. Ved utøvelsen av sin myndighet til å overvåke anvendelsen av denne artikkel og i samsvar med artikkel 11 i forordning (EU) 2019/1020 kan markedstilsynsmyndighetene utføre hensiktsmessige kontroller, særlig ved å ta hensyn til opplysninger som er lagret i EU-databasen nevnt i artikkel 71 i denne forordning.

Artikkel 81

Unionens beskyttelsesprosedyre

1. Dersom markedstilsynsmyndigheten i en medlemsstat innen tre måneder etter AV meldingen nevnt I artikkel 79 nr. 5, eller innen 30 dager forbudet mot ULOVLIG praksis nevnt i artikkel 5 ikke overholdes, gjør innvendinger mot et tiltak truffet av en annen markedstilsynsmyndighet, eller dersom Kommisjonen anser tiltaket for å være i strid med unionsretten, skal Kommisjonen uten ugrunnet opphold innlede samråd med markedstilsynsmyndigheten i den berørte medlemsstaten og den eller de driftsansvarlige, og skal evaluere det nasjonale tiltaket. På grunnlag av resultatene av denne evalueringen skal Kommisjonen innen seks måneder, eller innen 60 dager dersom forbudet mot ULOVLIG praksis nevnt i artikkel 5 ikke er overholdt, regnet fra underretningen nevnt i artikkel 79 nr. 5, avgjøre om det nasjonale tiltaket er berettiget, og skal markedstilsynsmyndigheten i den berørte medlemsstaten om sin beslutning. Kommisjonen skal også underrette alle andre markedstilsynsmyndigheter om sin beslutning.

2. Dersom Kommisjonen anser tiltaket truffet av den berørte medlemsstaten for å være berettiget, skal alle sikre at de treffer egnede restriktive tiltak med hensyn til det berørte alarmsystemet, f.eks. ved å kreve at alarmsystemet trekkes tilbake fra deres marked uten unødig opphold, og skal underrette Kommisjonen om dette. Dersom Kommisjonen anser det nasjonale tiltaket for å være uberettiget, skal den berørte medlemsstaten trekke tiltaket tilbake og underrette Kommisjonen om dette.

3. Dersom det nasjonale tiltaket anses som berettiget og det manglende samsvaret med AI-systemet tilskrives mangler ved de harmoniserte standardene eller felles spesifikasjonene nevnt i artikkel 40 og 41 i denne forordning, skal Kommisjonen anvende framgangsmåten fastsatt I artikkel 11 i forordning (EU) nr. 1025/2012.

Artikkel 82

AI-systemer som er kompatible og utgjør en risiko

1. Dersom markedstilsynsmyndigheten I en medlemsstat, etter å ha foretatt en vurdering i henhold til artikkel 79 og etter å ha rådført seg med den relevante nasjonale offentlige myndigheten nevnt I artikkel 77 nr. 1, finner at selv om et høyrisikosystem er i samsvar med denne forordning, utgjør det likevel en risiko for menneskers helse eller sikkerhet, for grunnleggende rettigheter eller for andre aspekter ved vern av allmenne interesser, skal den kreve at den relevante driftsansvarlige treffer alle hensiktsmessige tiltak for å sikre at det berørte AI-systemet, når det bringes i omsetning eller tas i bruk, ikke lenger utgjør en slik risiko, uten ugrunnet opphold og innen en frist som den kan fastsette.".

2. Tilbyderen eller en annen relevant aktør skal sikre at det treffes korrigerende tiltak med hensyn til alle de berørte AI-systemene som vedkommende har gjort tilgjengelig på unionsmarkedet, innen den tidsfristen som er fastsatt av markedstilsynsmyndigheten i den medlemsstaten som er nevnt i nr. 1.

3. Medlemsstatene skal umiddelbart underrette Kommisjonen og de andre medlemsstatene om en konklusjon i henhold til nr. 1. Denne informasjonen skal omfatte alle tilgjengelige opplysninger, særlig de data som er nødvendige for å identifisere det berørte KI-systemet, KI-SYSTEMETS opprinnelse og forsyningskjede, arten av den aktuelle risikoen og arten og varigheten av de nasjonale tiltakene som er truffet.

4. Kommisjonen skal uten ugrunnet opphold rådføre seg med de berørte medlemsstatene og de relevante driftsansvarlige og skal evaluere de nasjonale tiltakene som er truffet. På grunnlag av resultatene av denne evalueringen skal Kommisjonen avgjøre om tiltaket er berettiget, og om nødvendig foreslå andre egnede tiltak.

5. Kommisjonen skal umiddelbart underrette de berørte medlemsstatene og de relevante driftsansvarlige om sin beslutning. Den skal også underrette de øvrige medlemsstatene.

Artikkel 83

Formell manglende overholdelse

1. Dersom markedstilsynsmyndigheten i en medlemsstat gjør ett av følgende funn, skal den kreve at den aktuelle leverandøren bringer den manglende etterlevelsen til opphør innen en frist som den kan fastsette:

(a) CE-merkingen er påført i strid med artikkel 48;

(b) CE-merkingen ikke er påført;

(c) EU-samsvarserklæringen nevnt i artikkel 47 ikke er ;

(d) EU-samsvarserklæringen nevnt i artikkel 47 ikke er korrekt utformet;

(e) registreringen i EU-databasen nevnt i artikkel 71 ikke har blitt ;

(f) det ikke er oppnevnt noen fullmektig der det er aktuelt;

(g) teknisk dokumentasjon er ikke tilgjengelig.

2. Dersom den manglende oppfyllelsen av kravene nevnt i nr. 1 vedvarer, skal I den berørte medlemsstaten treffe egnede og forholdsmessige tiltak for å begrense eller forby at høyrisikosystemet gjøres tilgjengelig på markedet, eller for sikre at det tilbakekalles eller trekkes tilbake fra markedet uten forsinkelse.

Artikkel 84

Støttestrukturer for testing av AI i Unionen

1. Kommisjonen skal utpeke en eller flere av Unionens støttestrukturer for testing av AI til å utføre oppgavene oppført i artikkel 21 nr. 6 i forordning (EU) 2019/1020 på AI-OMRÅDET.

2. Uten at det berører oppgavene nevnt I nr. 1, skal Unionens støttestrukturer for testing også gi uavhengig teknisk eller vitenskapelig rådgivning på anmodning fra styret, Kommisjonen eller markedstilsynsmyndighetene.

AVSNITT 4

Rettsmidler

Artikkel 85

Rett til å klage til en markedsovervåkningsmyndighet

Uten at det berører andre administrative eller rettslige rettsmidler, kan enhver fysisk eller juridisk person som har grunn til å anta at det har funnet sted en overtredelse av bestemmelsene i denne forordning, inngi klage til den relevante markedstilsynsmyndigheten.

I samsvar med forordning (EU) 2019/1020 skal slike klager tas i betraktning i forbindelse med markedsovervåkingsaktiviteter, og skal håndteres i tråd med de særlige prosedyrene som markedsovervåkingsmyndighetene har etablert for dette.

Artikkel 86

Rett til forklaring av individuelle beslutninger

1. enhver berørt person som er gjenstand for en beslutning som er truffet av den driftsansvarlige PÅ grunnlag av resultatene FRA ET høyrisiko-AI-system oppført i vedlegg III, med unntak av systemer oppført I nr. 2, og som har rettsvirkninger eller på tilsvarende måte i betydelig grad påvirker vedkommende på en måte som vedkommende anser å ha en negativ innvirkning på helse, sikkerhet eller grunnleggende rettigheter, skal ha rett til å få klare og meningsfulle forklaringer fra den driftsansvarlige PÅ hvilken rolle AI-systemet har spilt i beslutningsprosedyren og hovedelementene I beslutningen som ER truffet.

2. Nr. 1 får ikke anvendelse på bruk AV AI-systemer for hvilke det I samsvar med unionsretten følger unntak fra eller begrensninger i forpliktelsen i henhold til nevnte nr. 1 i unionsretten eller nasjonal rett.

3. Denne artikkel får anvendelse bare i den utstrekning retten nevnt i nr. 1 ikke er fastsatt på annen måte unionsretten.

Artikkel 87

Rapportering av overtredelser og beskyttelse av personer som rapporterer

direktiv (EU) 2019/1937 skal gjelde for rapportering av overtredelser av denne forordning og beskyttelse av personer som rapporterer slike overtredelser.

AVSNITT 5

Tilsyn, etterforskning, håndheving og overvåking av leverandører av generelle AI-modeller

Artikkel 88

Håndheving av forpliktelsene til leverandører av generelle AI-modeller

1. Kommisjonen skal ha enekompetanse til å føre tilsyn med og håndheve kapittel V, idet det tas hensyn til de prosessuelle garantier i henhold til artikkel 94. Kommisjonen skal overlate gjennomføringen av disse oppgavene TIL AI-kontoret, uten at det berører Kommisjonens organisasjonsmyndighet og fordelingen av kompetanse mellom medlemsstatene og Unionen på grunnlag av traktatene.

2. Uten at det berører artikkel 75 nr. 3, kan markedstilsynsmyndighetene anmode Kommisjonen om å utøve de fullmakter som er fastsatt i denne avdeling, dersom det er nødvendig og forholdsmessig for å bistå dem i utførelsen av deres oppgaver i henhold til denne forordning.

Artikkel 89

Overvåking av tiltak

1. For å utføre oppgavene som er tillagt det I henhold til dette avsnitt, kan AI-kontoret treffe de nødvendige tiltak for å overvåke den effektive gjennomføringen og overholdelsen av denne forordning av leverandører av allmenne AI-modeller, herunder deres overholdelse av godkjente regler for god praksis.

2. nedstrømsleverandører skal ha rett til å inngi EN klage med påstand om brudd på denne forordning. en klage skal være behørig begrunnet og minst inneholde opplysninger om

(a) kontaktpunktet til leverandøren av den aktuelle generelle aI-modellen;

(b) en beskrivelse av de relevante fakta, de berørte bestemmelsene i denne forordning og årsaken til at nedstrømsleverandøren mener at leverandøren av den aktuelle allsidige AI-modellen har brutt denne forordning;

(c) all annen informasjon som nedstrømsleverandøren som har sendt forespørselen, anser som relevant, herunder, det er relevant, informasjon som er innhentet på eget initiativ.

Artikkel 90

Varsler om systemrisiko fra det vitenskapelige panelet

1. Det vitenskapelige panelet kan gi en kvalifisert advarsel TIL AI-kontoret dersom det har grunn til å mistenke at

(a) en generell AI-modell utgjør en konkret identifiserbar risiko på unionsnivå; eller

(b) en generell AI-modell oppfyller vilkårene nevnt I artikkel 51.

2. Ved en slik kvalifisert varsling kan Kommisjonen, gjennom AI-kontoret og etter å ha underrettet styret, utøve de fullmakter som er fastsatt i denne seksjon for å vurdere saken. AI-kontoret skal underrette Styret om ethvert tiltak i henhold til artikkel 91 til 94.

3. EN kvalifisert varsling skal være behørig begrunnet og minst angi:

(a) kontaktpunktet for leverandøren av den generelle aI-modellen med berørt systemrisiko;

(b) en beskrivelse av relevante fakta og begrunnelsen for det vitenskapelige panelets varsling;

(c) all annen informasjon som fagpanelet anser som relevant, herunder eventuelt informasjon som er innhentet på eget initiativ.

Artikkel 91

Myndighet til å be om dokumentasjon og informasjon

1. Kommisjonen kan anmode tilbyderen AV den berørte allsidige AI-modellen om å framlegge dokumentasjonen som er utarbeidet av tilbyderen i samsvar med artikkel 53 og 55, eller eventuelle tilleggsopplysninger som er nødvendige for å vurdere om tilbyderen overholder denne forordning.

2. Før aI-kontoret sender om informasjon, kan det innlede en strukturert dialog med leverandøren den generelle aI-modellen.

3. Etter en behørig begrunnet anmodning fra det vitenskapelige panelet kan Kommisjonen utstede en anmodning opplysninger til en leverandør av en generell KI-modell, dersom tilgangen til opplysninger er nødvendig og forholdsmessig for at det vitenskapelige panelet skal kunne utføre sine oppgaver i henhold til artikkel 68 nr. 2.

4. Anmodningen om opplysninger skal angi rettsgrunnlaget og formålet med anmodningen, spesifisere hvilke opplysninger som kreves, fastsette en frist for når opplysningene skal gis, og angi bøtene som er fastsatt i artikkel 101 for å gi uriktige, ufullstendige eller villedende opplysninger.

5. Tilbyderen AV den berørte allmenne KI-modellen eller dennes representant skal gi den informasjonen det anmodes om. Når gjelder juridiske personer, selskaper eller firmaer, eller dersom leverandøren ikke er en juridisk person, skal de personer som er bemyndiget til å representere dem i henhold til lov eller vedtekter, gi den etterspurte informasjonen på vegne av leverandøren av den aktuelle generelle aI-modellen. Advokater som er behørig bemyndiget til å opptre, kan gi opplysninger på vegne av sine klienter. Klientene skal likevel være fullt ut ansvarlige dersom opplysningene som gis, er ufullstendige, uriktige eller villedende.

Artikkel 92

Myndighet til å gjennomføre evalueringer

1. aI-kontoret kan, etter å ha rådført seg med styret, gjennomføre evalueringer av den aktuelle generelle aI-modellen:

(a) for å vurdere leverandørens overholdelse forpliktelsene i henhold til denne forordning, dersom informasjonen som er innhentet i henhold til artikkel 91 er utilstrekkelig; eller

(b) å undersøke systemrisikoer på unionsnivå for generelle KI-modeller med systemrisiko, særlig etter et kvalifisert varsel fra det vitenskapelige panelet i samsvar med artikkel 90 nr. 1 bokstav a).

2. Kommisjonen kan beslutte å oppnevne uavhengige eksperter til å foreta evalueringer på sine vegne, herunder fra det vitenskapelige panelet som er opprettet i henhold til artikkel 68. Uavhengige sakkyndige som oppnevnes for denne oppgaven, skal oppfylle kriteriene fastsatt i artikkel 68 nr. 2.

3. Ved anvendelsen av nr. 1 kan Kommisjonen anmode om tilgang til den berørte allsidige KI-modellen gjennom API-ER eller andre egnede tekniske midler og verktøy, herunder kildekode.

4. Innsynsbegjæringen skal angi rettsgrunnlaget, formålet med og begrunnelsen for begjæringen og fastsette fristen for å gi innsyn, samt bøtene som er fastsatt i artikkel 101 for unnlatelse av å gi innsyn.

5. Tilbyderne AV den berørte allmenne aI-modellen eller deres representant skal gi den informasjonen det anmodes om. Når gjelder juridiske personer, selskaper eller firmaer, eller dersom leverandøren ikke er en juridisk person, skal de personene som er bemyndiget til å representere dem i henhold til lov eller vedtekter, gi den etterspurte tilgangen PÅ vegne AV den berørte leverandøren av den generelle aI-modellen.

6. Kommisjonen skal vedta gjennomføringsrettsakter som fastsetter de nærmere ordningene og vilkårene for evalueringene, herunder de nærmere ordningene for involvering av uavhengige eksperter, og framgangsmåten for utvelgelse av disse. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten for behandling nevnt i artikkel 98 nr. 2.

7. Før aI-kontoret ber om tilgang til den aktuelle generelle AI-MODELLEN, kan aI-kontoret innlede en strukturert dialog med leverandøren av den generelle aI-modellen for å innhente mer informasjon om den interne testingen av modellen, interne sikkerhetstiltak for å forebygge systemrisiko og andre interne prosedyrer og tiltak som leverandøren har iverksatt for å redusere slik risiko.

Artikkel 93

Myndighet til å be om tiltak

1. Kommisjonen kan, der det er nødvendig og hensiktsmessig, anmode tilbyderne om å

(a) treffe egnede tiltak for å oppfylle forpliktelsene i artikkel 53 og 54;

(b) iverksette risikoreduserende tiltak dersom evalueringen som er utført i samsvar med artikkel 92, har gitt opphav til alvorlig og begrunnet bekymring for en systemrisiko på unionsnivå;

(c) begrense tilgjengeliggjøringen på markedet, trekke tilbake eller tilbakekalle modellen.

2. Før et tiltak blir etterspurt, kan aI-kontoret innlede en strukturert dialog med leverandøren av den generelle aI-modellen.

3. Dersom tilbyderen av den generelle aI-modellen med systemrisiko i løpet av den strukturerte dialogen nevnt i nr. 2 gir tilsagn om å gjennomføre risikoreduserende tiltak for å håndtere en systemrisiko på unionsplan, kan Kommisjonen ved beslutning gjøre disse tilsagnene bindende og erklære at det ikke er noen ytterligere grunn til å gripe inn.

Artikkel 94

Prosedyrerettigheter for økonomiske aktører i den generelle AI-modellen

artikkel 18 i forordning (EU) 2019/1020 får *tilsvarende* anvendelse på tilbydere av den generelle aI-modellen, uten at det berører mer spesifikke prosessuelle rettigheter fastsatt i denne forordning.

CHaPTER X

ETISKE REGLER OG RETNINGSLINJER

Artikkel 95

Adferdskodekser for frivillig anvendelse av spesifikke krav

1. AI-kontoret og medlemsstatene skal oppmuntre til og legge til rette for utarbeidelse av atferdsregler, herunder tilhørende styringsmekanismer, som skal fremme frivillig anvendelse på andre AI-SYSTEMER enn , av noen av eller alle kravene fastsatt i kapittel III avsnitt 2, idet det tas hensyn til tilgjengelige tekniske løsninger og beste praksis i bransjen som gjør det mulig å anvende slike krav.

2. AI-kontoret og medlemsstatene skal legge til rette for utarbeidelse av adferdskodekser for frivillig anvendelse, også av distributører, av spesifikke krav til alle AI-systemer, på grunnlag av klare mål og nøkkelindikatorer for å måle oppnåelsen av disse målene, herunder elementer som, men ikke begrenset til, følgende

(a) relevante elementer som er fastsatt i Unionens etiske retningslinjer for pålitelig AI;

(b) vurdere og minimere innvirkningen AV AI-systemer på miljømessig bærekraft, blant annet med hensyn til energieffektiv programmering og teknikker for effektiv utforming, opplæring og bruk av AI;

(c) fremme kunnskap om AI, særlig hos personer som arbeider med utvikling, drift og bruk AV AI;

(d) legge til rette for en inkluderende og mangfoldig utforming AV AI-systemer, blant annet ved å etablere inkluderende og mangfoldige utviklingsteam og fremme interessenters deltakelse i denne prosessen;

(e) vurdere og forebygge negative konsekvenser av AI-systemer for sårbare personer eller grupper av sårbare personer, blant annet når det gjelder tilgjengelighet for personer med nedsatt funksjonsevne, samt likestilling mellom kjønnene.

3. Adferdskodekser kan utarbeides av individuelle tilbydere eller brukere av AI-SYSTEMER eller av organisasjoner som representerer dem, eller av begge, herunder med deltakelse av alle interesserte interessenter og deres representative organisasjoner, herunder organisasjoner i det sivile samfunn og akademia. De etiske retningslinjene kan omfatte ett eller flere AI-SYSTEMER, idet det tas hensyn til likheten mellom de relevante systemenes tiltenkte formål.

4. AI-kontoret og medlemsstatene skal ta hensyn til de særlige interessene og behovene til små og mellomstore bedrifter, herunder nyetablerte bedrifter, når de oppmuntrer til og legger til rette for utarbeidelse av atferdsnormer.

Artikkel 96

Retningslinjer fra Kommisjonen om gjennomføringen av denne forordningen

1. Kommisjonen skal utarbeide retningslinjer for den praktiske gjennomføringen av denne forordning, og særlig om

(a) anvendelsen av kravene og forpliktelsene nevnt i artikkel 8 til 15 og i artikkel 25;

(b) de forbudte praksisene nevnt i artikkel 5;

(c) den praktiske gjennomføringen av bestemmelsene knyttet til vesentlige endringer;

(d) den praktiske gjennomføringen av åpenhetsforpliktelsene i artikkel 50;

(e) detaljert informasjon om forholdet mellom denne forordning og Unionens harmoniseringslovgivning oppført i vedlegg I, samt med annen relevant unionslovgivning, herunder med hensyn til konsekvens i håndhevingen av dem;

(f) anvendelse av definisjonen AV ET AI-system som angitt i artikkel 3 nr. 1.

Når Kommisjonen utsteder slike retningslinjer, skal den ta særlig hensyn til behovene til små og mellomstore bedrifter, herunder nyetablerte bedrifter, lokale offentlige myndigheter og de sektorene som mest sannsynlig vil bli berørt av denne forordning.

Retningslinjene nevnt I første ledd i dette nummer skal ta behørig hensyn til det allment anerkjente tekniske utviklingstrinn PÅ KI-OMRÅDET, samt til relevante harmoniserte standarder og felles spesifikasjoner som er nevnt i artikkel 40 og 41, eller til de harmoniserte standardene eller tekniske spesifikasjonene som er fastsatt i henhold til Unionens harmoniseringsregelverk.

2. på anmodning fra medlemsstatene eller aI-kontoret, eller på eget initiativ, skal Kommisjonen oppdatere tidligere vedtatte retningslinjer når den anser det nødvendig.

CHaPTER XI

DELEGERING AV MYNDIGHET OG KOMITÉPROSEDYRE

Artikkel 97

Utøvelse av delegasjonen

1. Kommisjonen gis myndighet til å vedta delegerte rettsakter på de vilkår som er fastsatt i denne artikkel.

2. Myndigheten til å vedta delegerte rettsakter nevnt i artikkel 6 . 6 og 7, artikkel 7 . 1 og 3, artikkel 11 nr. 3, artikkel 43 nr. 5 og 6, artikkel 47 nr. 5, artikkel 51 nr. 3, artikkel 52 nr. 4 og artikkel 53 . 5 og 6 skal gis til Kommisjonen for en periode på fem år fra og med 1. august 2024. Kommisjonen skal utarbeide en rapport om delegeringen av myndighet senest ni måneder før utløpet av femårsperioden. Delegeringen av myndighet skal stilltiende forlenges med perioder av samme varighet, med mindre Europaparlamentet eller Rådet motsetter seg en slik forlengelse senest tre måneder før utløpet av hver periode.

3. Delegeringen av myndighet nevnt i artikkel 6 nr. 6 og 7, artikkel 7 nr. 1 og 3, artikkel 11 nr. 3, ARTIKKEL 43 nr. 5 og 6, artikkel 47 nr. 5, artikkel 51 nr. 3, artikkel 52 nr. 4 og artikkel 53 nr 5 og 6 kan når som helst tilbakekalles av eller Rådet. et vedtak om tilbakekall skal bringe delegeringen av myndighet som er angitt i vedtaket, TIL opphør. Den får virkning dagen etter at den er kunngjort i *Den europeiske unions* tidende eller på et senere tidspunkt som er angitt i den. Den skal ikke berøre gyldigheten av delegerte rettsakter som allerede er trådt i kraft.

4. Før Kommisjonen vedtar en delegert rettsakt, skal den rådføre seg med eksperter utpekt av hver medlemsstat i samsvar med prinsippene fastsatt i den tverrinstitusjonelle avtalen av 13. april 2016 om bedre lovgivning.

5. så snart den vedtar en delegert rettsakt, skal Kommisjonen samtidig underrette Europaparlamentet og Rådet den.

6. enhver delegert rettsakt vedtatt i henhold til artikkel 6 nr. 6 eller 7, artikkel 7 nr. 1 eller 3, artikkel 11 nr. 3, ARTIKKEL 43 nr. 5 eller 6, artikkel 47 nr. 5, artikkel 51 nr. 3, artikkel 52 nr. 4 eller artikkel 53 nr. 5 eller 6 skal tre i kraft artikkel 52 nr. 4 eller artikkel 53 nr. 5 eller 6 trer i kraft bare dersom verken Europaparlamentet eller Rådet har gjort innsigelse innen en frist på tre måneder etter at rettsakten er meddelt Europaparlamentet og Rådet, eller dersom både Europaparlamentet og Rådet før av denne fristen har underrettet Kommisjonen om at de ikke vil gjøre innsigelse. Fristen skal forlenges med tre måneder på initiativ fra Europaparlamentet eller Rådet.

Artikkel 98

Komitéprosedyre

1. Kommisjonen skal bistås av en komité. Denne komité skal være en komité i henhold til forordning (EU) nr. 182/2011.

2. Når det henvises til dette ledd, får artikkel 5 i forordning (EU) nr. 182/2011 anvendelse.

CHaPTER XII

STRAFF

Artikkel 99

Straff

1. I samsvar med vilkårene og betingelsene fastsatt i denne forordning skal medlemsstatene fastsette regler om sanksjoner og andre håndhevingstiltak, som også kan omfatte advarsler og ikke-monetære tiltak, som skal gjelde for driftsansvarliges overtredelser av denne forordning, og skal treffe alle nødvendige tiltak for å sikre at de gjennomføres på en korrekt og effektiv måte, idet de tar hensyn til de retningslinjer som Kommisjonen har utstedt i henhold til artikkel 96. De fastsatte sanksjonene skal være effektive, forholdsmessige og avskrekkende. De skal ta hensyn til interessene til små og mellomstore bedrifter, herunder nyetablerte bedrifter, og deres økonomiske levedyktighet.

2. Medlemsstatene skal uten opphold og senest innen datoen for ikrafttredelse underrette Kommisjonen om reglene om sanksjoner og andre håndhevingstiltak nevnt i nr. 1, og skal uten opphold underrette Kommisjonen om eventuelle senere endringer av dem.

3. Overtredelse av forbudet mot ULOVLIG praksis nevnt I artikkel 5 skal straffes med administrative bøter på inntil 35 000 000 EUR eller, dersom overtrederen er et foretak, inntil 7 % av foretakets samlede årlige omsetning på verdensbasis i det foregående regnskapsåret, avhengig av HVA som er høyest.

4. Overtredelse av noen av følgende bestemmelser knyttet til driftsansvarlige eller meldte organer, bortsett fra dem som er fastsatt i artikkel 5, skal medføre administrative bøter på opptil 15 000 000 EUR eller, dersom overtrederen er et foretak, opptil 3 % av foretakets samlede årlige omsetning på verdensbasis for det foregående regnskapsåret, avhengig av hva som er høyest:

(a) leverandørens forpliktelser i henhold til artikkel 16;

(b) fullmektigenes forpliktelser i henhold til artikkel 22;

(c) importørers forpliktelser i henhold til artikkel 23;

(d) distributørers forpliktelser i henhold til artikkel 24;

(e) forpliktelser for utplasserere i henhold til artikkel 26;

(f) krav og forpliktelser for meldte organer i henhold til artikkel 31, artikkel 33 . 1, 3 og 4 eller artikkel 34;

(g) åpenhetsforpliktelser for tilbydere og distributører i henhold til artikkel 50.

5. Dersom det gis uriktige, ufullstendige eller villedende opplysninger meldte organer eller nasjonale vedkommende myndigheter som svar på en anmodning, skal det ilegges administrative bøter på inntil 7 500 000 euro eller, dersom overtrederen er et foretak, 1 % av foretakets samlede årsomsetning på verdensbasis for det foregående regnskapsåret, avhengig av hva som er høyest.

6. For små og mellomstore bedrifter, herunder nyetablerte bedrifter, skal hver bot nevnt i denne artikkelen være opp til prosentandelen eller beløpet nevnt i nr. 3, 4 og 5, avhengig av hvilket av disse som er lavest.

7. Ved avgjørelsen av om det skal ilegges et overtredelsesgebyr og ved fastsettelsen av størrelsen på overtredelsesgebyret i hvert enkelt tilfelle, skal det tas hensyn til alle relevante omstendigheter i den konkrete situasjonen, og det skal, der det er hensiktsmessig, tas hensyn til følgende

(a) overtredelsens art, alvorlighetsgrad og varighet og konsekvensene av den, idet det tas hensyn til formålet MED AI-systemet, samt, der det er relevant, antall berørte personer og omfanget av skaden de har lidd;

(b) om andre markedsovervåkingsmyndigheter allerede har ilagt administrative bøter til den samme aktøren for samme overtredelse;

(c) om andre myndigheter allerede har ilagt den samme aktøren administrative bøter for overtredelser av annen unionsrett eller nasjonal rett, når slike overtredelser skyldes samme aktivitet eller unnlatelse som utgjør en relevant overtredelse av denne forordning;

(d) størrelsen, den årlige omsetningen og markedsandelen til aktøren som begår overtredelsen;

(e) eventuelle andre skjerpende eller formildende omstendigheter som er relevante for omstendighetene i saken, for eksempel økonomiske fordeler som er oppnådd, eller tap som er unngått, direkte eller indirekte, som følge av overtredelsen;

(f) graden av samarbeid med nasjonale vedkommende myndigheter for å avhjelpe overtredelsen og redusere de mulige negative virkningene av overtredelsen;

(g) graden av ansvar hos operatøren, med hensyn til de tekniske og organisatoriske tiltakene som operatøren har iverksatt;

(h) måten overtredelsen ble kjent for de nasjonale vedkommende myndigheter, særlig om, og i så fall i hvilken grad, den driftsansvarlige har meldt fra om overtredelsen;

(i) overtredelsens forsettlige eller uaktsomme karakter;

(j) eventuelle tiltak som operatøren har iverksatt for å redusere skaden som de berørte personene har lidd.

8. Hver medlemsstat skal fastsette regler om i hvilken utstrekning offentlige myndigheter og organer som er etablert i medlemsstaten, kan ilegges administrative bøter.

9. Avhengig av medlemsstatenes rettssystem kan reglene om administrative bøter anvendes på en slik måte at bøtene ilegges av kompetente nasjonale domstoler eller av andre organer, alt etter hva som gjelder i disse medlemsstatene. Anvendelsen av slike regler i disse medlemsstatene skal ha tilsvarende virkning.

10. Utøvelsen av myndighet i henhold til denne artikkel skal være underlagt egnede rettssikkerhetsgarantier i samsvar med unionsretten og nasjonal rett, herunder effektive rettsmidler og rettferdig rettergang.

11. Medlemsstatene skal hvert år rapportere til Kommisjonen om de administrative bøter de har utstedt i løpet av det året, i samsvar med denne artikkel, og om eventuelle tilknyttede tvister eller rettslige prosesser.

Artikkel 100

Administrative bøter for Unionens institusjoner, organer, kontorer og byråer

1. Den europeiske datatilsynsmann kan ilegge unionsinstitusjoner, -organer, -kontorer og -byråer som omfattes av denne forordning, administrative bøter. Ved avgjørelsen av om det skal ilegges et overtredelsesgebyr og ved fastsettelsen av på overtredelsesgebyret i hvert enkelt tilfelle, skal det tas hensyn til alle relevante omstendigheter i den konkrete situasjonen, og det skal tas behørig hensyn til følgende

(a) overtredelsens art, alvorlighetsgrad og varighet og dens konsekvenser, idet det tas hensyn til formålet det berørte AI-systemet, samt, der det er relevant, antallet berørte personer og omfanget av den skade de har lidd;

(b) graden av ansvar for unionsinstitusjonen, -organet, -kontoret eller -byrået, idet det tas hensyn til tekniske og organisatoriske tiltak som de har iverksatt;

(c) ethvert tiltak som Unionens institusjon, organ, kontor eller byrå har truffet for å avbøte skaden som de berørte personene har lidd;

(d) graden av samarbeid med Den europeiske DATATILSYNSMANN for å avhjelpe overtredelsen og redusere de mulige negative virkningene av overtredelsen, herunder etterlevelse av tiltak som Den europeiske datatilsynsmann tidligere har pålagt den berørte unionsinstitusjonen, det berørte unionsorganet, det berørte unionsbyrået eller den berørte unionsinstitusjonen, det berørte unionsinstansen, det berørte unionsorganet, det berørte unionsorganet eller det berørte unionsbyrået med hensyn til det samme saksforholdet;

(e) eventuelle lignende tidligere overtredelser begått av Unionens institusjon, organ, kontor eller byrå;

(f) måten overtredelsen ble kjent for Den europeiske datatilsynsmann, særlig om, og i så fall i hvilken utstrekning, unionsinstitusjonen, -organet, -kontoret eller -byrået meldte fra om overtredelsen;

(g) det årlige budsjettet til Unionens institusjon, organ, kontor eller byrå.

2. Overtredelse av forbudet mot ULOVLIG praksis nevnt I artikkel 5 skal straffes med administrative bøter på inntil 1 500 000 euro.

3. DERSOM aI-systemet ikke oppfyller andre krav eller forpliktelser i henhold til denne forordning enn de som er fastsatt i artikkel 5, skal det ilegges administrative bøter på opptil 750 000 euro.

4. Før Den europeiske DATATILSYNSMANN treffer beslutninger i henhold til denne artikkel, skal Den europeiske datatilsynsmann gi unionsinstitusjonen, -organet, -kontoret eller -byrået som er gjenstand for Den europeiske datatilsynsmanns saksbehandling, mulighet til å bli hørt i saken om den mulige overtredelsen. Den europeiske skal basere sine beslutninger bare på elementer og omstendigheter som de berørte parter har hatt anledning til å uttale seg om. Eventuelle klagere skal være nært knyttet til saksbehandlingen.

5. De berørte partenes rett til kontradiksjon skal respekteres fullt ut under saksbehandlingen. De skal ha rett til innsyn i Den europeiske datatilsynsmannens saksmappe, med forbehold om enkeltpersoners eller foretaks berettigede interesse i å beskytte sine personopplysninger eller forretningshemmeligheter.

6. Midler som innkreves ved ileggelse av bøter i henhold til denne artikkel, skal bidra til Unionens alminnelige budsjett. Bøtene skal ikke påvirke den effektive driften av Unionens institusjon, organ, kontor eller byrå som er ilagt bøter.

7. Det europeiske datatilsynet skal hvert år underrette Kommisjonen om de administrative bøter det har ilagt i henhold til denne artikkel, og om eventuelle søksmål eller rettssaker det har innledet.

Artikkel 101

Bøter for leverandører av generelle AI-modeller

1. Kommisjonen kan ilegge tilbydere av allmenne AI-modeller bøter som ikke overstiger 3 % av deres samlede årlige omsetning på verdensbasis i det foregående regnskapsåret eller 15 000 000 EUR, avhengig av hvilket beløp som er høyest, dersom Kommisjonen finner at tilbyderen har opptrådt forsettlig eller uaktsomt:

(a) overtrådt de relevante bestemmelsene i denne forordning;

(b) unnlatt å etterkomme en anmodning om et dokument eller om opplysninger i henhold til artikkel 91, eller gitt uriktige, ufullstendige eller villedende opplysninger;

(c) ikke har etterkommet en anmodning om tiltak i henhold til artikkel 93;

(d) unnlatt å gi Kommisjonen tilgang til den generelle AI-modellen eller den GENERELLE AI-modellen med systemrisiko med henblikk på å gjennomføre en evaluering i henhold til artikkel 92.

Ved fastsettelsen av bøttens eller tvangsmulktens skal det tas hensyn til overtredelsens art, alvorlighetsgrad og varighet, idet det tas behørig hensyn til prinsippene om forholdsmessighet og hensiktsmessighet. Kommisjonen skal også ta hensyn til tilsagn som er gitt i samsvar med artikkel 93 nr. 3, eller som er gitt i relevante regler for god praksis i samsvar med artikkel 56.

2. Før Kommisjonen treffer vedtak i henhold til nr. 1, skal den underrette leverandøren av generelle aI-modellen om sine foreløpige konklusjoner og gi vedkommende mulighet til å bli hørt.

3. Bøter som ilegges i henhold til denne artikkel, skal være effektive, forholdsmessige og avskrekkende.

4. Informasjon om bøter som ilegges i henhold til denne paragrafen, skal også formidles til styret etter behov.

5. Den europeiske unions domstol skal ha ubegrenset kompetanse til å prøve Kommisjonens beslutninger om fastsettelse av bøter i henhold til denne artikkel. Den kan oppheve, nedsette eller forhøye den ilagte boten.

6. Kommisjonen skal vedta gjennomføringsrettsakter som inneholder nærmere bestemmelser og rettssikkerhetsgarantier for saksbehandlingen med henblikk på eventuell vedtakelse av beslutninger i henhold til nr. 1 i denne artikkel. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten for behandling nevnt i artikkel 98 nr. 2.

CHaPTER XIII

ENDELIGE BESTEMMELSER

Artikkel 102

Endring av forordning (EF) nr. 300/2008

I artikkel 4 nr. 3 i forordning (EF) nr. 300/2008 skal følgende ledd tilføyes

"Når det vedtas detaljerte tiltak knyttet til tekniske spesifikasjoner og framgangsmåter for godkjenning og bruk av sikkerhetsutstyr som gjelder systemer for kunstig intelligens i henhold til europaparlaments- og rådsforordning (EU) nr. 2024/1689 (*), .skal det tas hensyn til kravene fastsatt i kapittel III avsnitt 2 i nevnte forordning

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler om kunstig intelligens og om endring av forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU 2018/1139 og (EU) 2019/2144 og direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (lov om kunstig intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj).".

Artikkel 103

Endring av forordning (EU) nr. 167/2013

I artikkel 17 nr. 5 i forordning (EU) nr. 167/2013 skal følgende ledd tilføyes

"Ved vedtakelse av delegerte i henhold til første ledd vedrørende systemer for kunstig intelligens som sikkerhetskomponenter i henhold til europaparlaments- og rådsforordning (EU nr. 2024/1689 (*), skal det tas hensyn til kravene fastsatt i kapittel III avsnitt 2 i nevnte forordning.

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler om kunstig intelligens og om endring av forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU 2018/1139 og (EU) 2019/2144 og direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (lov om kunstig intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj).".

Artikkel 104

Endring av forordning (EU) nr. 168/2013

I artikkel 22 nr. 5 i forordning (EU) nr. 168/2013 skal følgende ledd tilføyes

"Ved vedtakelse av delegerte rettsakter i henhold til første ledd vedrørende systemer for kunstig intelligens som er sikkerhetskomponenter i henhold til europaparlaments- og rådsforordning (EU nr. 2024/1689 (*), skal kravene fastsatt i kapittel III avsnitt 2 i nevnte forordning tas i betraktning.

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler om kunstig intelligens og om endring av forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU 2018/1139 og (EU) 2019/2144 og direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (lov om kunstig intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj).".

Artikkel 105

Endring av direktiv 2014/90/EU

I artikkel 8 i direktiv 2014/90/EU skal følgende ledd legges til:

"5. Når det gjelder systemer for kunstig intelligens som er sikkerhetskomponenter i henhold til europaparlaments- og rådsforordning (*), EU) nr. 2024/1689 av (skal Kommisjonen, når den utøver sin virksomhet i henhold til nr. 1 og vedtar tekniske spesifikasjoner og prøvingsstandarder i samsvar med nr. 2 og 3, ta hensyn til kravene fastsatt i kapittel III avsnitt 2 i nevnte forordning.

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler om kunstig intelligens og om endring av forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU 2018/1139 og (EU) 2019/2144 og direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (lov om kunstig intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj).".

Artikkel 106

Endring av direktiv (EU) 2016/797

I artikkel 5 i direktiv (EU) 2016/797 skal følgende ledd legges til:

'12. Ved vedtakelse av delegerte rettsakter i henhold til nr. 1 og gjennomføringsrettsakter i henhold nr. 11 vedrørende systemer for kunstig intelligens som er sikkerhetskomponenter i henhold til europaparlaments- og rådsforordning (*).EU) nr. 2024/1689 (, skal det tas hensyn til kravene fastsatt i kapittel III avsnitt 2 i nevnte forordning

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler om kunstig intelligens og om endring av forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU 2018/1139 og (EU) 2019/2144 og direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (lov om kunstig intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj).".

Artikkel 107

Endring av forordning (EU) 2018/858

I artikkel 5 i forordning (EU) 2018/858 skal følgende ledd legges til

'4. Ved vedtakelse av delegerte rettsakter i henhold til nr. 3 vedrørende systemer for kunstig intelligens som er sikkerhetskomponenter i henhold til europaparlaments- og rådsforordning (EU 2024/1689 (*), skal det tas hensyn til kravene fastsatt i kapittel III avsnitt 2 i nevnte forordning.

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler om kunstig intelligens og om endring av forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU 2018/1139 og (EU) 2019/2144 og direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (lov om kunstig intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj).".

Artikkel 108

Endringer i forordning (EU) 2018/1139

I forordning (EU) 2018/1139 gjøres følgende endringer

(1) I artikkel 17 tilføyes følgende avsnitt:

'3. Uten at det berører nr. 2, skal det ved vedtakelse av gjennomføringsrettsakter i henhold til nr. 1 om systemer for kunstig intelligens som er sikkerhetskomponenter i henhold til europaparlaments- og rådsforordning (EU) nr. 2024/1689 (*), .tas hensyn til kravene fastsatt i kapittel III avsnitt 2 i nevnte forordning

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler om kunstig intelligens og om endring av forordning (EFnr. 300/2008, (EUnr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2019/2144 og direktiv 2014/90/EU, (EU) 2016/797.
og (EU) 2020/1828 (lov om kunstig intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).";

(2) I artikkel 19 tilføyes følgende avsnitt:

"4. Ved vedtakelse av delegerte rettsakter i henhold til nr. 1 og 2 vedrørende systemer for kunstig intelligens som er sikkerhetskomponenter i henhold til forordning (EU) nr. 2024/1689, skal det tas hensyn til kravene fastsatt i kapittel III avsnitt 2 i nevnte forordning.";

(3) I artikkel 43 tilføyes følgende avsnitt:

'4. Ved vedtakelse av gjennomføringsrettsakter i henhold til nr. 1 om systemer for kunstig intelligens som er sikkerhetskomponenter i henhold til forordning (EU) nr. 2024/1689, skal det tas hensyn til kravene fastsatt i kapittel III avsnitt 2 i nevnte forordning.";

(4) I artikkel 47 tilføyes følgende avsnitt:

"3. Ved vedtakelse av delegerte rettsakter i henhold til nr. 1 og 2 vedrørende systemer for kunstig intelligens som er sikkerhetskomponenter i henhold til forordning (EU) nr. 2024/1689, skal det tas hensyn til kravene fastsatt i kapittel III avsnitt 2 i nevnte forordning.";

(5) I artikkel 57 skal følgende ledd tilføyes

"Ved vedtakelsen av disse gjennomføringsrettsaktene om systemer for kunstig intelligens som sikkerhetskomponenter i henhold til forordning (EU) nr. 2024/1689, skal det tas hensyn til kravene fastsatt i kapittel III avsnitt 2 i nevnte forordning.";

(6) I artikkel 58 tilføyes følgende avsnitt:

"3. Ved vedtakelse av delegerte rettsakter i henhold til nr. 1 og 2 vedrørende systemer for kunstig intelligens som er sikkerhetskomponenter i henhold til forordning (EU) nr. 2024/1689, skal det tas hensyn til kravene fastsatt i kapittel III avsnitt 2 i nevnte forordning.".

Artikkel 109

Endring av forordning (EU) 2019/2144

I artikkel 11 i forordning (EU) 2019/2144 skal følgende ledd legges til:

'3. Ved vedtakelsen av gjennomføringsrettsaktene i henhold til nr. 2 vedrørende systemer for kunstig intelligens som er sikkerhetskomponenter i henhold til europaparlaments- og rådsforordning (EU2024/1689 (*), skal det tas hensyn til kravene fastsatt i kapittel III avsnitt 2 i nevnte forordning.

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler om kunstig intelligens og om endring av forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU 2018/1139 og (EU) 2019/2144 og direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (lov om kunstig intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj).".

Artikkel 110

Endring av direktiv (EU) 2020/1828

I vedlegg I til europaparlaments- og rådsdirektiv (EU) 2020/1828 ([58]) tilføyes følgende punkt

"(68) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler om kunstig intelligens og om endring av forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2019/2144 og direktiv 2014/90/EU, (EU) 2016/797 og EU) 2020/1828 (lov om kunstig intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj).".

Artikkel 111

AI-systemer som allerede er markedsført eller tatt i bruk, og generelle AI-modeller som allerede er markedsført

1. Uten at det berører anvendelsen av artikkel 5 som nevnt i artikkel 113 nr. 3 bokstav a), skal AI-SYSTEMER som er komponenter de store IT-systemene som er etablert ved rettsaktene oppført i vedlegg X, og som er brakt I omsetning eller tatt i bruk før 2. august 2027, bringes I samsvar med denne forordning senest 31. desember 2030.

Kravene fastsatt i denne forordning skal tas i betraktning ved evalueringen av alle store IT-systemer som er opprettet ved rettsaktene oppført i vedlegg X, og som skal foretas som fastsatt i disse rettsaktene og når disse erstattes eller endres.

2. Uten at det berører anvendelsen av artikkel 5 som nevnt i artikkel 113 nr. 3 bokstav a), får denne forordning anvendelse på operatører AV andre høyrisiko-AI-systemer enn systemene nevnt i nr. 1 i denne artikkel, som er brakt i omsetning eller tatt i bruk før 2. august 2026, bare dersom disse systemene fra og med nevnte dato er gjenstand for vesentlige endringer i utformingen. Under alle omstendigheter skal leverandører og utplasserere av høyrisikosystemer FOR KUNSTIG INTELLIGENS SOM er beregnet å brukes av offentlige myndigheter, treffe de nødvendige tiltak for å oppfylle kravene og forpliktelsene i denne forordning innen 2. august 2030.

3. Leverandører av allsidige aI-modeller som er brakt i omsetning før 2. august 2025, skal treffe de nødvendige å oppfylle forpliktelsene fastsatt i denne forordning innen 2. august 2027.

(58) Europaparlaments- og rådsdirektiv (EU) 2020/1828 av 25. november 2020 om representative tiltak for beskyttelse av forbrukernes kollektive interesser og om oppheving av direktiv 2009/22/EF (EUT L 409 av 4.12.2020, s. 1).

Artikkel 112

Evaluering og gjennomgang

1. Kommisjonen skal vurdere behovet for å endre listen i vedlegg III og listen forbudt praksis fastsatt I artikkel 5 én gang i året etter at denne forordning har trådt i kraft, og fram til utløpet AV perioden for delegering av myndighet fastsatt i artikkel 97. Kommisjonen skal framlegge resultatene av denne vurderingen for Europaparlamentet og Rådet.

2. Innen 2. august 2028 og deretter hvert fjerde år skal Kommisjonen evaluere og rapportere til Europaparlamentet og Rådet om følgende

(a) behovet for endringer som utvider eksisterende områdeoverskrifter eller legger til nye områdeoverskrifter i vedlegg III;

(b) endringer I listen OVER AI-systemer som krever ytterligere åpenhetstiltak i artikkel 50;

(c) endringer som øker effektiviteten i tilsyns- og styringssystemet.

3. Innen 2. august 2029 og deretter hvert fjerde år skal Kommisjonen framlegge en rapport om evalueringen og gjennomgangen av denne forordning for Europaparlamentet og Rådet. Rapporten skal inneholde en vurdering håndhevingsstrukturen og det eventuelle behovet for et unionsorgan for å avhjelpe eventuelle identifiserte mangler. På grunnlag konklusjonene skal rapporten, dersom det er hensiktsmessig, ledsages av et forslag til endring av denne forordning. Rapportene skal offentliggjøres.

4. I rapportene nevnt i nr. 2 skal det tas særlig hensyn til følgende

(a) status for de nasjonale vedkommende myndigheters økonomiske, tekniske og menneskelige ressurser for effektivt å kunne utføre de oppgavene de er pålagt i henhold til denne forordning;

(b) sanksjonsnivået, særlig administrative bøter som nevnt i artikkel 99 nr. 1, som anvendes av medlemsstatene for overtredelser av denne forordning;

(c) vedtatt harmoniserte standarder og felles spesifikasjoner som er utviklet for å støtte denne forordningen;

(d) antall foretak som kommer inn markedet etter at denne forordning trer i kraft, og hvor mange av dem som er små og mellomstore bedrifter.

5. Innen 2. august 2028 skal Kommisjonen evaluere hvordan AI-kontoret fungerer, om AI-KONTORET har fått tilstrekkelige fullmakter og kompetanse til å utføre sine oppgaver, og om det vil være relevant og nødvendig for en korrekt gjennomføring og håndheving av denne forordning å oppgradere AI-KONTORET og dets håndhevingskompetanse og å øke dets ressurser. Kommisjonen skal framlegge en rapport om sin evaluering for Europaparlamentet og Rådet.

6. Innen 2. august 2028 og deretter hvert fjerde år skal Kommisjonen framlegge en rapport om gjennomgangen av framdriften I utviklingen AV standardiseringsleveranser om energieffektiv utvikling av allsidige KI-modeller og vurdere behovet for ytterligere tiltak eller handlinger, herunder bindende tiltak eller handlinger. Rapporten skal framlegges for Europaparlamentet og Rådet, og den skal offentliggjøres.

7. Innen 2. august 2028 og deretter hvert tredje år skal Kommisjonen evaluere virkningen og effektiviteten av frivillige atferdsnormer for å fremme anvendelsen av kravene fastsatt i kapittel III avsnitt 2 for andre AI-systemer enn høyrisiko-AI-systemer og eventuelt andre tilleggskrav for andre AI-SYSTEMER enn , herunder med hensyn til miljømessig bærekraft.

8. Ved anvendelsen av nr. 1-7 skal styret, medlemsstatene og nasjonale vedkommende myndigheter gi Kommisjonen opplysninger på Kommisjonens anmodning og uten ugrunnet opphold.

9. Ved gjennomføringen av evalueringene og gjennomgåelsene nevnt i nr. 1-7 skal Kommisjonen ta hensyn til standpunktene og konklusjonene fra styret, , Rådet og andre relevante organer eller kilder.

10. Kommisjonen skal om nødvendig legge fram hensiktsmessige forslag til endring av denne forordning, særlig med hensyn til den teknologiske utviklingen, AI-systemenes innvirkning på helse og sikkerhet og på grunnleggende rettigheter, og i lys av utviklingen i informasjonssamfunnet.

11. For å veilede evalueringene og gjennomgangene nevnt i nr. 1 til 7 i denne artikkel, skal AI-kontoret seg å utvikle en objektiv og deltakende metodikk for evaluering av risikonivåer basert på kriteriene som er skissert i de relevante artiklene, og inkludering av nye systemer i:

(a) listen i vedlegg III, herunder utvidelse av eksisterende områdeoverskrifter eller tilføyelse av nye områdeoverskrifter i nevnte vedlegg;

(b) listen over forbudte praksiser i artikkel 5; og

(c) listen OVER AI-systemer som krever ytterligere åpenhetstiltak I henhold til artikkel 50.

12. Enhver endring av denne forordning i henhold til nr. 10, eller relevante delegerte rettsakter eller gjennomføringsrettsakter, som gjelder sektorspesifikk EU-harmoniseringslovgivning oppført i avsnitt B i vedlegg I, skal ta hensyn til de særlige reguleringsmessige forholdene i hver sektor og de eksisterende styrings-, samsvarsvurderings- og håndhevingsmekanismene og -myndighetene som er etablert der.

13. Senest 2. august 2031 skal Kommisjonen foreta en vurdering av håndhevingen av denne forordning og rapportere om den til Europaparlamentet, Rådet og Den europeiske økonomiske og sosiale komité, idet det tas hensyn til de første årene denne forordning har vært anvendt. På grunnlag av resultatene skal rapporten, dersom det er hensiktsmessig, ledsages av et forslag til endring av denne forordning med hensyn til håndhevingsstrukturen og behovet et unionsbyrå for å avhjelpe eventuelle identifiserte mangler.

Artikkel 113

Ikrafttredelse og anvendelse

Denne forordning trer i kraft den tjuende dag etter at den er kunngjort i *Den europeiske unions tidende*.

Den skal gjelde fra 2. august 2026. Det er

imidlertid ikke mulig:

(a) Kapittel I og II får anvendelse fra 2. februar 2025;

(b) Kapittel III avsnitt 4, kapittel Vkapittel VII og kapittel XII og artikkel 78 skal gjelde fra 2. august 2025, med unntak av artikkel 101;

(c) artikkel 6 nr. 1 og de tilsvarende forpliktelsene i denne forordning skal gjelde fra 2. august 2027.

Denne forordning er bindende i alle enkeltsaker og får direkte anvendelse i alle . utferdiget i Brussel 13.

juni 2024.

På vegne av Europaparlamentet	*På Rådets vegne*
Presidenten	*Presidenten*
R. METSOLA	M. MICHEL

BILAG I

Liste over Unionens harmoniseringslovgivning

Del A. Liste over Unionens harmoniseringslovgivning basert på det nye lovgivningsrammeverket

1. Europaparlaments- og rådsdirektiv 2006/42/EF av 17. mai 2006 om maskiner og om endring av direktiv 95/16/EF (EUT L 157 av 9.6.2006, s. 24);

2. Europaparlaments- og rådsdirektiv 2009/48/EF av 18. juni 2009 om sikkerhet ved leketøy (EUT L 170 av 30.6.2009, s. 1);

3. Europaparlaments- og rådsdirektiv 2013/53/EU av 20. november 2013 om fritidsfartøyer og vannscootere og om oppheving av direktiv 94/25/EF (EUT L 354 av 28.12.2013, s. 90);

4. Europaparlaments- og rådsdirektiv 2014/33/EU av 26. februar 2014 om harmonisering av medlemsstatenes lovgivning om heiser og sikkerhetskomponenter til heiser (EUT L 96 av 29.3.2014, s. 251);

5. Europaparlaments- og rådsdirektiv 2014/34/EU av 26. februar 2014 om harmonisering av medlemsstatenes lovgivning om utstyr og sikringssystemer beregnet for bruk i eksplosjonsfarlig område (EUT L 96 av 29.3.2014, s. 309);

6. Europaparlaments- og rådsdirektiv 2014/53/EU av 16. april 2014 om harmonisering av medlemsstatenes lovgivning om tilgjengeliggjøring av radioutstyr på markedet og om oppheving av direktiv 1999/5/EF (EUT L 153 av 22.5.2014, s. 62);

7. Europaparlaments- og rådsdirektiv 2014/68/EU av 15. mai 2014 om harmonisering av medlemsstatenes lovgivning om tilgjengeliggjøring på markedet av trykkpåkjent utstyr (EUT L 189 av 27.6.2014, s. 164);

8. Europaparlaments- og rådsforordning (EU) 2016/424 av 9. mars 2016 om taubaneanlegg og om oppheving av direktiv 2000/9/EF (EUT L 81 av 31.3.2016, s. 1);

9. Europaparlaments- og rådsforordning (EU) 2016/425 av 9. mars 2016 om personlig verneutstyr og om oppheving av rådsdirektiv 89/686/EØF (EUT L 81 av 31.3.2016, s. 51);

10. Europaparlaments- og rådsforordning (EU) 2016/426 av 9. mars 2016 om apparater som bruker gassformig brensel og om oppheving av direktiv 2009/142/EF (EUT L 81 av 31.3.2016, s. 99);

11. Europaparlaments- og rådsforordning (EU) 2017/745 av 5. april 2017 om medisinsk utstyr, om endring av direktiv 2001/83/EF, forordning (EF) nr. 178/2002 og forordning (EF) nr. 1223/2009 og om oppheving av rådsdirektiv 90/385/EØF og 93/42/EØF (EUT L 117 av 5.5.2017, s. 1);

12. Europaparlaments- og rådsforordning (EU) 2017/746 av 5. april 2017 om medisinsk utstyr til *in* vitro-diagnostikk og om oppheving av direktiv 98/79/EF og kommisjonsbeslutning 2010/227/EU (EUT L 117 av 5.5.2017, s. 176).

Del B. Liste over annen EU-harmoniseringslovgivning

13. Europaparlaments- og rådsforordning (EF) nr. 300/2008 av 11. mars 2008 om felles bestemmelser om sikkerhet innen sivil luftfart og om oppheving av forordning (EF) nr. 2320/2002 (EUT L 97 av 9.4.2008, s. 72);

14. Europaparlaments- og rådsforordning (EU) nr. 168/2013 av 15. januar 2013 om godkjenning og markedstilsyn av to- og trehjulede kjøretøyer og firehjulinger (EUT L 60 av 2.3.2013, s. 52);

15. Europaparlaments- og rådsforordning (EU) nr. 167/2013 av 5. februar 2013 om godkjenning og markedstilsyn av landbruks- og skogbrukskjøretøyer (EUT L 60 av 2.3.2013, s. 1);

16. Europaparlaments- og rådsdirektiv 2014/90/EU av 23. juli 2014 om skipsutstyr og om oppheving av rådsdirektiv 96/98/EF (EUT L 257 av 28.8.2014, s. 146);

17. Europaparlaments- og rådsdirektiv (EU) 2016/797 av 11. mai 2016 om i jernbanesystemet i Den europeiske union (EUT L 138 av 26.5.2016, s. 44);

18. Europaparlaments- og rådsforordning (EU) 2018/858 av 30. mai 2018 om godkjenning og markedstilsyn av motorvogner og tilhengere til disse og av systemer, komponenter og separate tekniske enheter beregnet på slike kjøretøyer, om endring av forordning (EF) nr. 715/2007 og (EF) nr. 595/2009 og om oppheving av direktiv 2007/46/EF (EUT L 151 av 14.6.2018, s. 1);

19. Europaparlaments- og rådsforordning (EU) 2019/2144 av 27. november 2019 om krav til typegodkjenning av motorvogner og tilhengere til disse, og systemer, komponenter og separate tekniske enheter beregnet på slike kjøretøyer, med hensyn til deres generelle sikkerhet og beskyttelse av kjøretøyets passasjerer og myke trafikanter, endring av europaparlaments- og rådsforordning (EU) 2018/858 og om oppheving av forordning (EF) nr. 78/2009, (EF) nr. 79/2009 og (EF) nr. 661/2009 og kommisjonsforordning (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. 1008/2010, (EU) nr. 1009/2010, (EUnr. 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 av 16.12.2019, p. 1);

20. Europaparlaments- og rådsforordning (EU) 2018/1139 av 4. juli 2018 om felles regler for sivil luftfart og om opprettelse av Den europeiske unions byrå for luftfartssikkerhet, og om endring av forordning (EF) nr. 2111/2005, (EF) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 og europaparlaments- og rådsdirektiv 2014/30/EU og 2014/53/EU, og om oppheving av europaparlaments- og rådsforordning (EF) nr. 552/2004 og (EF) nr. 216/2008 og rådsforordning (EØF) nr. 3922/91 (EUT L 212 av 22.8.2018, s. 1), for så vidt gjelder konstruksjon, produksjon og omsetning av luftfartøyer nevnt i artikkel 2 nr. 1 a) og b) i nevnte forordning, når det gjelder ubemannede luftfartøyer og deres motorer, propeller, deler og utstyr for fjernstyring av dem.

BILAG II

Liste over straffbare handlinger nevnt i artikkel 5 nr. 1 første ledd bokstav h) nr. iii)

Straffbare handlinger som nevnt i artikkel 5 nr. 1 første ledd bokstav h) nr. iii):

— terrorisme,

— ,

— seksuell utnyttelse av barn og barnepornografi,

— ulovlig handel med narkotika eller psykotrope stoffer,

— ulovlig handel med våpen, ammunisjon eller eksplosiver,

— drap, grov legemsbeskadigelse,

— ulovlig handel med menneskelige organer eller vev,

— ulovlig handel med kjernefysisk eller radioaktivt materiale,

— kidnapping, ulovlig tvang eller gisseltaking,

— forbrytelser som faller inn under Den internasjonale straffedomstolens jurisdiksjon,

— ulovlig beslagleggelse av fly eller skip,

— voldtekt,

— miljøkriminalitet,

— organisert eller væpnet ran,

— sabotasje,

— deltakelse i en kriminell organisasjon som er involvert i en eller flere av lovbruddene nevnt ovenfor.

BILAG III

AI-systemer med høy risiko som nevnt i artikkel 6 nr. 2

Høyrisiko aI-systemer I henhold til artikkel 6(2) ER aI-systemer som er oppført på noen av følgende områder:

1. Biometri, i den grad bruken av dette er tillatt i henhold til relevant unionsrett eller nasjonal rett:

   (a) fjernstyrte biometriske identifikasjonssystemer.

   Dette skal ikke omfatte AI-systemer som er ment å brukes til biometrisk verifisering, OG hvis eneste formål er å bekrefte at en bestemt fysisk person er den personen han eller hun utgir seg for å være;

   (b) aI-systemer som er ment å brukes til biometrisk kategorisering i henhold til sensitive eller beskyttede attributter eller kjennetegn basert på utledning av disse attributtene eller kjennetegnene;

   (c) aI-systemer som skal brukes til følelsesgjenkjenning.

2. Kritisk infrastruktur: KI-systemer som skal brukes som sikkerhetskomponenter i styring og drift av kritisk digital infrastruktur, veitrafikk eller i forsyningen av vann, gass, varme eller elektrisitet.

3. Utdanning og yrkesopplæring:

   (a) aI-systemer som er ment å brukes til Å bestemme adgang eller opptak eller til å tildele fysiske personer adgang til utdannings- og yrkesopplæringsinstitusjoner på alle nivåer;

   (b) aI-systemer som skal brukes til å evaluere læringsutbytte, inkludert når dette utbyttet brukes til å styre læringsprosessen til fysiske personer i utdannings- og yrkesopplæringsinstitusjoner på alle nivåer;

   (c) aI-systemer som skal brukes til å vurdere hvilket utdanningsnivå en person vil få eller vil kunne få tilgang til, i forbindelse med eller innenfor utdannings- og yrkesopplæringsinstitusjoner på alle nivåer;

   (d) aI-systemer som skal brukes til å overvåke og oppdage forbudt atferd hos studenter under prøver i forbindelse med eller innenfor utdannings- og yrkesopplæringsinstitusjoner på alle nivåer.

4. Sysselsetting, arbeidsledelse og adgang til selvstendig næringsvirksomhet:

   (a) aI-systemer som skal brukes til rekruttering eller utvelgelse av fysiske personer, særlig for å legge ut målrettede stillingsannonser, analysere og filtrere jobbsøknader og vurdere kandidater;

   (b) aI-systemer som er ment å brukes til Å ta beslutninger som påvirker vilkårene for arbeidsrelaterte relasjoner, forfremmelse eller avslutning av arbeidsrelaterte kontraktsforhold, til å tildele oppgaver basert på individuell atferd eller personlige trekk eller egenskaper, eller til å overvåke og evaluere prestasjoner og atferd hos personer i slike relasjoner.

5. tilgang til og utnyttelse av viktige private tjenester og viktige offentlige tjenester og goder:

   (a) aI-systemer som er ment å brukes av offentlige myndigheter eller på vegne av offentlige myndigheter for å vurdere fysiske personers berettigelse til viktige offentlige ytelser og tjenester, herunder helsetjenester, samt for å innvilge, redusere, tilbakekalle eller kreve tilbake slike ytelser og tjenester;

   (b) KI-systemer som er ment å brukes til å vurdere kredittverdigheten til fysiske personer eller fastsette deres kredittverdighet, med unntak av KI-systemer som brukes til å avdekke økonomiske misligheter;

   (c) aI-systemer som skal brukes til risikovurdering og prising i forhold til fysiske personer når det gjelder livs- og helseforsikring;

(d) aI systemer som er beregnet på å evaluere og klassifisere nødanrop fra fysiske personer, eller som skal brukes til å sende ut, eller til å fastsette prioritet utsendelse av, førstehjelpstjenester, herunder av politi, brannmenn og medisinsk hjelp, samt systemer for triagering av akuttpasienter i helsevesenet.

6. rettshåndhevelse, i den grad bruken av dem er tillatt i henhold til relevant unionsrett eller nasjonal rett:

(a) aI-systemer som er ment å brukes av eller på vegne av rettshåndhevende myndigheter, eller av Unionens institusjoner, organer, kontorer eller byråer til støtte for rettshåndhevende myndigheter eller på deres vegne, for å vurdere risikoen for at en fysisk person blir offer for straffbare handlinger;

(b) AI-systemer som er beregnet på Å brukes av eller på vegne rettshåndhevende myndigheter eller av Unionens institusjoner, organer, kontorer eller byråer til støtte for rettshåndhevende myndigheter som løgndetektorer eller lignende verktøy;

(c) aI-systemer SOM skal brukes av eller på vegne rettshåndhevende myndigheter, eller av Unionens institusjoner, organer, kontorer eller byråer, til støtte for rettshåndhevende myndigheter for å vurdere pålitelighetenav bevis i forbindelse med etterforskning eller straffeforfølgning av straffbare handlinger;

(d) aI-systemer som er beregnet på å brukes av rettshåndhevende myndigheter eller på deres vegne eller av Unionens institusjoner, organer, kontorer eller byråer til støtte for rettshåndhevende myndigheter for å vurdere risikoen at en fysisk person begår lovbrudd eller begår nye lovbrudd, ikke utelukkende på grunnlag av profilering av fysiske personer som nevnt i artikkel 3 nr. 4 i direktiv (EU) 2016/680, eller for å vurdere personlighetstrekk og karakteristika eller tidligere kriminell atferd hos fysiske personer eller grupper;

(e) aI-systemer som er beregnet på Å brukes av eller på vegne rettshåndhevende myndigheter eller av Unionens institusjoner, organer, kontorer eller byråer til støtte for rettshåndhevende myndigheter til profilering av fysiske personer som nevnt i artikkel 3 nr. 4 i direktiv (EU) 2016/680 i forbindelse med avsløring, etterforskning eller rettsforfølgning av straffbare handlinger.

7. Migrasjon, asyl og grensekontroll, i den grad bruken av dem er tillatt i henhold til relevant unionsrett eller nasjonal rett:

(a) AI-systemer som er beregnet på Å bli brukt av eller på vegne av vedkommende offentlige myndigheter eller av Unionens institusjoner, organer, kontorer eller byråer som løgndetektorer eller lignende verktøy;

(b) aI-systemer som er beregnet på Å brukes av eller på vegne av vedkommende offentlige myndigheter eller av Unionens institusjoner, organer, kontorer eller byråer for å vurdere en risiko, herunder en sikkerhetsrisiko, en risiko for irregulær migrasjon eller en helserisiko, som utgjøres av en fysisk person som har hensikt å reise inn på eller som har reist inn på en territorium;

(c) aI-systemer som er beregnet på Å brukes av eller på vegne av vedkommende offentlige myndigheter eller av Unionens institusjoner, organer, kontorer eller byråer for å bistå vedkommende offentlige myndigheter I behandlingen av søknader om asyl, visum eller oppholdstillatelse og for tilknyttede klager med hensyn til om de fysiske personene som om en status, er kvalifisert, herunder tilknyttede vurderinger av bevisenes pålitelighet;

(d) aI-systemer som er beregnet på Å brukes av eller på vegne av vedkommende offentlige myndigheter, eller av Unionens institusjoner, organer, kontorer eller byråer, i forbindelse med migrasjons-, asyl- eller grensekontrollforvaltning, med det formål å oppdage, gjenkjenne eller identifisere fysiske personer, med unntak av verifisering av reisedokumenter.

8. rettspleie og demokratiske prosesser:

(a) aI-systemer som er ment å brukes av en rettslig myndighet eller på deres vegne for å bistå en rettslig myndighet med å undersøke og tolke fakta og lov og anvende loven på et konkret sett med fakta, eller for å brukes på en lignende måte i alternativ tvisteløsning;

(b) AI-SYSTEMER som er ment å brukes til å påvirke utfallet av et valg eller en folkeavstemning eller fysiske personers stemmegivning i forbindelse med valg eller folkeavstemninger. Dette omfatter ikke AI-systemer som fysiske personer ikke er direkte eksponert for, for eksempel verktøy som brukes til å organisere, optimalisere eller strukturere politiske kampanjer fra et administrativt eller logistisk synspunkt.

BILAG IV

Teknisk dokumentasjon nevnt i artikkel 11 nr. 1

Den tekniske dokumentasjonen nevnt i artikkel 11 nr. 1 skal minst inneholde følgende opplysninger, alt etter hva som gjelder for det aktuelle AI-systemet:

1. EN generell beskrivelse AV AI-systemet, inkludert:

   (a) det tiltenkte formålet, navnet på leverandøren og versjonen av systemet som gjenspeiler forholdet til tidligere versjoner;

   (b) hvordan aI-systemet samhandler med, eller kan brukes til å samhandle med, maskinvare eller programvare, inkludert med andre aI-systemer, som ikke er en del av selve aI-systemet, der det er aktuelt;

   (c) versjonene av relevant programvare eller fastvare, og eventuelle krav knyttet til versjonsoppdateringer;

   (d) beskrivelse av alle former som AI-systemet markedsføres eller tas i bruk i, for eksempel programvarepakker som er innebygd i maskinvare, nedlastinger ELLER API-ER;

   (e) beskrivelse av maskinvaren SOM AI-systemet er ment å kjøre på;

   (f) der AI-systemet er en del av produkter, fotografier eller illustrasjoner som viser ytre kjennetegn, merking og innvendig utforming av disse produktene;

   (g) en grunnleggende beskrivelse av brukergrensesnittet som tilbys til utrulleren;

   (h) bruksanvisninger for utrulleren, og en grunnleggende beskrivelse av brukergrensesnittet som leveres til utrulleren, der det er aktuelt;

2. en detaljert beskrivelse av elementene I KI-systemet og av prosessen for utviklingen av det, inkludert

   (a) metodene og trinnene som er utført for å utvikle AI-systemet, herunder, der det er relevant, av forhåndsprogrammerte systemer eller verktøy levert av tredjeparter, og hvordan disse ble brukt, integrert eller modifisert av leverandøren;

   (b) systemets designspesifikasjoner, dvs. den generelle logikken I KI-systemet og algoritmene; de viktigste designvalgene, herunder begrunnelsen og forutsetningene som er gjort, blant annet med hensyn til personer eller grupper av personer som systemet ment å skulle brukes på; de viktigste klassifiseringsvalgene; hva systemet er utformet for å optimalisere for, og relevansen av de ulike parameterne; beskrivelsen av systemets forventede resultat og resultatkvalitet; beslutningene om eventuelle avveininger som er gjort med hensyn til de tekniske løsningene som er valgt for å oppfylle kravene fastsatt i kapittel III, avsnitt 2;

   (c) beskrivelse av systemarkitekturen som forklarer hvordan programvarekomponentene bygger på eller griper inn i hverandre og integreres I den samlede prosesseringen; beregningsressursene som brukes til å utvikle, trene, teste og validere AI-systemet;

   (d) der det er relevant, datakravene i form av dataark som beskriver opplæringsmetodene og -teknikkene og opplæringsdatasettene som brukes, inkludert en generell beskrivelse av disse datasettene, informasjon om hvor de kommer fra, omfang og hovedegenskaper, hvordan dataene ble innhentet og valgt ut, merkingsprosedyrer (f.eks. for veiledet læring), datarensningsmetoder (f.eks. påvisning av ekstremverdier);

   (e) vurdering av de menneskelige tilsynstiltakene som er nødvendige i samsvar med artikkel 14, herunder en vurdering de tekniske tiltakene som er nødvendige for å gjøre det lettere for utbyggerne å tolke resultatene fra KI-systemene, I samsvar med artikkel 13 nr. 3 bokstav d);

   (f) der det er relevant, en detaljert beskrivelse av forhåndsbestemte endringer i KI-systemet og dets ytelse, sammen med all relevant informasjon om de tekniske løsningene som er tatt i bruk for å sikre at KI-systemet kontinuerlig oppfyller de relevante kravene i kapittel III, avsnitt 2;

   (g) validerings- og testprosedyrene som er brukt, herunder informasjon om validerings- og testdataene som er brukt, og deres viktigste egenskaper; beregninger som er brukt for å måle nøyaktighet, robusthet og samsvar med andre relevante krav fastsatt i kapittel III, avsnitt 2, samt potensielt diskriminerende virkninger; testlogger og alle testrapporter datert og signert av de ansvarlige personene, herunder med hensyn til forhåndsdefinerte endringer som nevnt i bokstav f);

(h) cybersikkerhetstiltak på plass;

3. detaljert informasjon om overvåking, funksjon og kontroll AV KI-systemet, særlig med hensyn til dets kapasitet og begrensninger i ytelse, herunder graden av nøyaktighet for bestemte personer eller grupper av personer som systemet er ment å brukes på, og det generelle forventede nøyaktighetsnivået i forhold til det tiltenkte formålet; de forutsigbare utilsiktede resultatene og kildene til risikoer for helse og sikkerhet, grunnleggende rettigheter og diskriminering i lys av det tiltenkte formålet med AI-SYSTEMET; de menneskelige tilsynstiltakene som er nødvendige i samsvar med artikkel 14, herunder de tekniske tiltakene som er innført for å lette tolkningen av aI-systemenes resultater for dem som tar dem i bruk; spesifikasjoner for inngangsdata, der det er relevant;

4. EN beskrivelse av ytelsesmålenes egnethet for det spesifikke AI-systemet;

5. en detaljert beskrivelse av risikostyringssystemet i samsvar med artikkel 9;

6. EN beskrivelse av relevante endringer som leverandøren har gjort i systemet gjennom dets livssyklus;

7. en liste over de harmoniserte standardene som er anvendt helt eller delvis, og hvis referanser er offentliggjort i *Den europeiske unions tidende*; dersom slike harmoniserte standarder ikke er anvendt, en detaljert beskrivelse av de løsninger som er valgt for å oppfylle kravene i kapittel III, avsnitt 2, herunder en liste over andre relevante standarder og tekniske spesifikasjoner som er anvendt;

8. EN kopi av EU-samsvarserklæringen nevnt i artikkel 47;

9. en detaljert beskrivelse av systemet som er etablert for å evaluere KI-systemets ytelse I fasen etter at det er brakt i omsetning i samsvar med artikkel 72, herunder planen for overvåking etter at utstyret er brakt I omsetning, jf. artikkel 72 nr. 3.

BILAG V

EU-samsvarserklæring

EU-samsvarserklæringen nevnt i artikkel 47 skal inneholde alle følgende opplysninger

1. aI-systemets navn og type og eventuelle andre entydige referanser som gjør det mulig å identifisere og spore AI-SYSTEMET;
2. Navn og adresse til leverandøren eller, der det er aktuelt, til deres autoriserte representant;
3. EN erklæring om at EU-samsvarserklæringen nevnt i artikkel 47 er utstedt på leverandørens eneansvar;
4. EN erklæring om AT AI-systemet er I samsvar med denne forordning , dersom det ER relevant, med annen relevant unionslovgivning som utstedelse av EU-samsvarserklæringen nevnt i artikkel 47;
5. Når et AI-system innebærer behandling av personopplysninger, en erklæring om AT AI-systemet er i samsvar forordning (EU) 2016/679 og (EU) 2018/1725 og direktiv (EU) 2016/680;
6. Referanser til relevante harmoniserte standarder som brukes eller andre felles spesifikasjoner som det erklæres samsvar i forhold ;
7. Eventuelt navn og identifikasjonsnummer på det meldte organet, en beskrivelse av samsvarsvurderingsprosedyren som er utført, og identifikasjon av sertifikatet som er utstedt;
8. Sted og dato for utstedelse av erklæringen, navn og funksjon til den personen som har undertegnet den, samt en angivelse av for hvem eller på vegne av hvem vedkommende har undertegnet, en underskrift.

BILAG VI

Prosedyre for samsvarsvurdering basert på internkontroll

1. Prosedyren for samsvarsvurdering basert på internkontroll er prosedyren for samsvarsvurdering basert på punkt 2, 3 og 4.

2. Tilbyderen verifiserer at det etablerte kvalitetsstyringssystemet er i samsvar med kravene i artikkel 17.

3. Leverandøren undersøker informasjonen i den tekniske dokumentasjonen for å vurdere om KI-systemet er i samsvar med de relevante grunnleggende kravene som er fastsatt i kapittel III, avsnitt 2.

4. Leverandøren verifiserer også at design- og utviklingsprosessen FOR KI-systemet og overvåkingen av det etter at det er brakt i omsetning, som nevnt i artikkel 72, er i samsvar med den tekniske dokumentasjonen.

BILAG VII

Samsvar basert på vurdering av kvalitetsstyringssystemet og en vurdering av den tekniske dokumentasjonen

1. Innledning

Samsvar basert på en vurdering av kvalitetsstyringssystemet og en vurdering av den tekniske dokumentasjonen er prosedyren for samsvarsvurdering basert på punkt 2 til 5.

2. Oversikt

Det godkjente kvalitetsstyringssystemet for konstruksjon, utvikling og prøving av KI-systemer I henhold til artikkel 17 skal undersøkes I samsvar med nr. 3 og skal være gjenstand for tilsyn som angitt i nr. 5. Den tekniske dokumentasjonen AV KI-systemet skal undersøkes i samsvar med nr. 4.

3. Kvalitetsstyringssystem

3.1. Tilbyderens søknad skal inneholde:

(a) navn adresse på tilbyderen og, dersom søknaden er innlevert av en autorisert representant, også dennes navn og adresse;

(b) listen OVER AI-systemer som dekkes av det samme ;

(c) den tekniske dokumentasjonen for hvert AI-system som omfattes av det samme ;

(d) dokumentasjonen om kvalitetsstyringssystemet, som skal dekke alle aspektene som er nevnt i artikkel 17;

(e) en beskrivelse av prosedyrene som skal sikre at kvalitetsstyringssystemet forblir tilstrekkelig og effektivt;

(f) en skriftlig erklæring om at den samme søknaden ikke er inngitt til noe annet meldt organ.

3.2. Kvalitetsstyringssystemet skal vurderes av det meldte organet, som skal avgjøre om det oppfyller kravene nevnt i artikkel 17.

Avgjørelsen skal meddeles leverandøren eller dennes representant.

Meldingen skal inneholde konklusjonene fra vurderingen av kvalitetsstyringssystemet og en begrunnet beslutning om vurderingen.

3.3. Det godkjente kvalitetsstyringssystemet skal fortsatt implementeres og vedlikeholdes av leverandøren, slik at det forblir tilstrekkelig og effektivt.

3.4. enhver planlagt endring I det godkjente kvalitetsstyringssystemet eller I listen OVER AI-systemer som omfattes av dette, skal leverandøren underrette det meldte organet om dette.

De foreslåtte endringene skal undersøkes av det meldte organet, som skal avgjøre om det endrede kvalitetsstyringssystemet fortsatt oppfyller kravene nevnt i punkt 3.2, eller om det er nødvendig med en ny vurdering.

Det meldte organet skal underrette leverandøren om sin beslutning. Meldingen skal inneholde konklusjonene fra gjennomgangen av endringene og den begrunnede vurderingsavgjørelsen.

4. Kontroll av den tekniske dokumentasjonen.

4.1. I tillegg til søknaden nevnt i nr. 3 skal leverandøren inngi en søknad til et meldt organ etter eget valg om vurdering av den tekniske dokumentasjonen for det AI-systemet som leverandøren har til hensikt å bringe I omsetning eller ta i bruk, og som omfattes av nevnt i nr. 3.

4.2. Søknaden skal inneholde:

(a) navn og adresse til leverandøren;

(b) en skriftlig erklæring om at den samme søknaden ikke er inngitt til noe annet meldt organ;

(c) den tekniske dokumentasjonen som er nevnt i vedlegg IV.

4.3. Den tekniske dokumentasjonen skal undersøkes av det meldte organet. Når det er relevant, og begrenset til det som er nødvendig for at det skal kunne utføre sine oppgaver, skal det meldte organet gis full tilgang til de opplærings-, valideringS- og testdatasettene som brukes, herunder, der det er hensiktsmessig og underlagt sikkerhetstiltak, gjennom API eller andre relevante tekniske midler og verktøy som muliggjør fjerntilgang.

4.4. Ved gjennomgangen AV den tekniske dokumentasjonen kan det meldte organet kreve at leverandøren fremlegger ytterligere dokumentasjon eller utfører ytterligere prøvinger for å gjøre det mulig å foreta en korrekt vurdering av OM KI-systemet er i samsvar med kravene fastsatt i kapittel III avsnitt 2. Dersom det meldte organet ikke er tilfreds med de prøvingene som er utført av leverandøren, skal det meldte organet selv utføre tilstrekkelige prøvinger, alt etter hva som er hensiktsmessig.

4.5. Dersom det er nødvendig for å vurdere om høyrisiko-indikatorsystemet er i samsvar med kravene fastsatt i kapittel III avsnitt 2, etter at alle andre rimelige metoder for å verifisere samsvar er uttømt og har vist seg å være utilstrekkelige, skal det meldte organet PÅ begrunnet anmodning også gis tilgang til opplæring og opplærte modeller AV indikatorsystemet, herunder dets relevante parametere. Slik tilgang skal være underlagt gjeldende unionsrett om vern av immaterielle rettigheter og forretningshemmeligheter.

4.6. Det meldte organets beslutning skal meddeles leverandøren eller dennes representant. Meldingen skal inneholde konklusjonene av vurderingen av den tekniske dokumentasjonen og den begrunnede vurderingsavgjørelsen.

Dersom KI-systemet er I samsvar med kravene fastsatt i kapittel III avsnitt 2, skal det meldte organet utstede et unionssertifikat for vurdering av teknisk dokumentasjon. Sertifikatet skal inneholde leverandørens navn og adressekonklusjonene av undersøkelsen, eventuelle vilkår for sertifikatets gyldighet og de opplysningene som er nødvendige for å identifisere aI-systemet.

Sertifikatet og dets vedlegg skal inneholde alle relevante opplysninger som gjør det mulig å vurdere om KI-systemet er I samsvar med kravene, og å kontrollere KI-systemet mens det er i bruk, der det er aktuelt.

Dersom AI-systemet ikke er i samsvar med kravene fastsatt i kapittel III avsnitt 2, skal det meldte organet avslå å utstede et unionssertifikat for vurdering av teknisk dokumentasjon og skal underrette søkeren om dette og gi en detaljert begrunnelse for avslaget.

Dersom KI-systemet ikke oppfyller kravet til dataene som er brukt til å lære det opp, må læres opp på nytt før det kan søkes om en ny samsvarsvurdering. I dette tilfellet skal den begrunnede vurderingsavgjørelsen fra det meldte organet som nekter å utstede Unionens sertifikat for vurdering av teknisk dokumentasjon, inneholde spesifikke betraktninger om kvalitetsdataene som er brukt til å trene opp KI-systemet, særlig om årsakene til manglende samsvar.

4.7. enhver endring av KI-systemet som kan påvirke KI-systemets samsvar med kravene eller dets tiltenkte formål, skal vurderes av det meldte organet som har utstedt Unionens sertifikat for vurdering av teknisk dokumentasjon. Leverandøren skal underrette det meldte organet om sin intensjon om å innføre noen av de ovennevnte endringene, eller hvis han på annen måte blir oppmerksom på at slike endringer vil forekomme. De planlagte endringene skal vurderes av det meldte organet, som skal avgjøre om disse endringene krever en ny samsvarsvurdering i samsvar med artikkel 43 nr. 4, eller om de kan håndteres ved hjelp av et tillegg til Unionens sertifikat for vurdering av teknisk dokumentasjon. I sistnevnte tilfelle skal det meldte organet vurdere endringene, underrette leverandøren om sin beslutning og, dersom endringene godkjennes, utstede et tillegg til Unionens sertifikat for vurdering av teknisk dokumentasjon til leverandøren.

5. Overvåking av det godkjente kvalitetsstyringssystemet.

5.1. Formålet med kontrollen som utføres av det meldte organet nevnt i punkt 3, er å sikre at leverandøren oppfyller vilkårene og betingelsene i det godkjente kvalitetsstyringssystemet.

5.2. For vurderingsformål skal leverandøren gi det meldte organet adgang til lokalene der konstruksjon, utvikling og testing AV AI-systemene finner sted. Tilbyderen skal videre dele all nødvendig informasjon med det meldte organet.

5.3. Det meldte organet skal gjennomføre periodiske revisjoner for å sikre at leverandøren opprettholder og anvender kvalitetsstyringssystemet, og skal gi leverandøren en revisjonsrapport. I forbindelse med disse revisjonene kan det meldte organet utføre ytterligere prøvinger AV DE AI-systemene som det er utstedt et unionssertifikat for vurdering av teknisk dokumentasjon for.

BILAG VIII

Informasjon som skal sendes inn ved registrering av høyrisiko AI-systemer i samsvar med artikkel 49

Del A - Opplysninger som skal fremlegges av tilbydere AV høyrisiko-AI-systemer I samsvar med artikkel 49(1)

Følgende informasjon skal gis og deretter holdes oppdatert med hensyn til høyrisikosystemer som registreres i samsvar med artikkel 49(1):

1. Navn, adresse og kontaktinformasjon til leverandøren;

2. Dersom innlevering av informasjon utføres av en annen person på vegne av leverandøren, skal denne personens navn, adresse og kontaktopplysninger oppgis;

3. Navn, adresse og kontaktopplysninger til den autoriserte representanten, der det er aktuelt;

4. aI-systemets handelsnavn og enhver annen entydig referanse som gjør det mulig å identifisere og spore AI-SYSTEMET;

5. en beskrivelse av det tiltenkte formålet med aI-systemet og av komponentene og funksjonene som støttes gjennom dette aI-systemet;

6. EN grunnleggende og kortfattet beskrivelse av informasjonen som brukes av systemet (data, inndata) og dets driftslogikk;

7. Status FOR AI-systemet (PÅ markedet eller i bruk; ikke lenger på markedet/i bruk, tilbakekalt);

8. Type, nummer og utløpsdato for sertifikatet som er utstedt av det meldte organet, og eventuelt det meldte organets navn eller identifikasjonsnummer;

9. en skannet kopi av sertifikatet nevnt i punkt 8, der det er relevant;

10. enhver medlemsstat der AI-systemet er brakt I omsetning, tatt i bruk eller gjort tilgjengelig i Unionen;

11. EN kopi av EU-samsvarserklæringen nevnt i artikkel 47;

12. Elektroniske bruksanvisninger; denne informasjonen skal ikke gis for høyrisikosystemer på områdene rettshåndhevelse eller migrasjons-, asyl- og grensekontrollforvaltning som nevnt i vedlegg III nr. 1, 6 og 7;

13. EN URL for ytterligere informasjon (valgfritt).

Del B - Informasjon som skal sendes inn AV leverandører AV høyrisiko-AI-systemer I samsvar med artikkel 49(2)

Følgende informasjon skal gis og deretter holdes oppdatert med hensyn til AI-systemer som skal registreres i samsvar med artikkel 49(2):

1. Navn, adresse og kontaktinformasjon til leverandøren;

2. Dersom innlevering av informasjon utføres av en annen person på vegne av leverandøren, skal denne personens navn, adresse og kontaktopplysninger oppgis;

3. Navn, adresse og kontaktopplysninger til den autoriserte representanten, der det er aktuelt;

4. aI-systemets handelsnavn og eventuelle andre entydige referanser som gjør det mulig å identifisere og spore AI-SYSTEMET;

5. EN beskrivelse av det tiltenkte formålet med AI-systemet;

6. Betingelsen eller betingelsene i henhold til artikkel 6(3) som ligger til grunn for AT AI-systemet ikke anses å være høyrisiko;

7. ET kort sammendrag av begrunnelsen FOR AT AI-systemet ikke anses å utgjøre en høy risiko i henhold til prosedyren i artikkel 6(3);

8. Status FOR AI-systemet (PÅ markedet eller i bruk; ikke lenger på markedet/i bruk, tilbakekalt);

9. enhver medlemsstat der AI-systemet er brakt I omsetning, tatt i bruk eller gjort tilgjengelig i Unionen.

Del C - Informasjon som skal sendes inn av utbyggere AV høyrisiko-AI-systemer I samsvar med artikkel 49(3)

Følgende informasjon skal gis og deretter holdes oppdatert med hensyn til høyrisikosystemer som registreres i henhold til artikkel 49 nr. 3:

1. Navn, adresse og kontaktinformasjon til den som distribuerer;
2. Navn, adresse og kontaktinformasjon til den personen som sender inn informasjon på vegne av utstederen;
3. URL-adressen til leverandørens oppføring AV aI-systemet i EU-databasen;
4. ET sammendrag av resultatene av konsekvensutredningen om grunnleggende rettigheter som er gjennomført i samsvar med artikkel 27;
5. ET sammendrag av konsekvensanalysen for personvern som er utført i samsvar med artikkel 35 i forordning (EU) 2016/679 eller artikkel 27 i direktiv (EU) 2016/680 som angitt i artikkel 26 nr. 8 i denne forordning, der det er relevant.

BILAG IX

Informasjon som skal sendes inn ved registrering av høyrisikosystemer for kunstig intelligens oppført i vedlegg III i forbindelse med testing under reelle forhold i samsvar med artikkel 60

Følgende informasjon skal gis og deretter holdes oppdatert med hensyn til testing under reelle forhold som skal registreres i henhold til artikkel 60:

1. ET unionsomfattende unikt identifikasjonsnummer for testing under reelle forhold;
2. Navn og kontaktinformasjon til leverandøren eller den potensielle leverandøren og til de som er involvert i testingen under reelle forhold;
3. EN kort beskrivelse AV AI-systemet, dets tiltenkte formål og annen informasjon som er nødvendig for å systemet;
4. ET sammendrag av de viktigste egenskapene ved planen for testing under reelle forhold;
5. Informasjon om avbrytelse eller avslutning av testingen under reelle forhold.

BILAG X

Unionens rettsakter om store IT-systemer på området frihet, sikkerhet og rettferdighet

1. Schengens informasjonssystem

(a) Europaparlaments- og rådsforordning (EU) 2018/1860 av 28. november 2018 om bruk av Schengen-informasjonssystemet for retur av tredjelandsborgere med ulovlig opphold (EUT L 312 av 7.12.2018, s. 1).

(b) Europaparlaments- og rådsforordning (EU) 2018/1861 av 28. november 2018 om opprettelse, drift og bruk av Schengen-informasjonssystemet (SIS) i forbindelse med grensekontroll, og om endring av konvensjonen om gjennomføring av Schengen-avtalen, og om endring og oppheving av forordning (EF) nr. 1987/2006 (EUT L 312 av 7.12.2018, s. 14).

(c) Europaparlaments- og rådsforordning (EU) 2018/1862 av 28. november 2018 om opprettelse, drift og bruk av Schengen-informasjonssystemet (SIS) på området politisamarbeid og strafferettslig samarbeid, om endring og oppheving av rådsbeslutning 2007/533/JHA og om oppheving av europaparlaments- og rådsforordning (EF) nr. 1986/2006 og kommisjonsbeslutning 2010/261/EU (EUT L 312 av 7.12.2018, s. 56).

2. Visuminformasjonssystem

(a) Europaparlaments- og rådsforordning (EU) 2021/1133 av 7. juli 2021 om endring av forordning (EU) nr. 603/2013, EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 og (EU) 2019/818 med hensyn til fastsettelse av vilkårene for tilgang til andre EU-informasjonssystemer med henblikk på visuminformasjonssystemet (EUT L 248 av 13.7.2021, s. 1).

(b) Europaparlaments- og rådsforordning (EU) 2021/1134 av 7. juli 2021 om endring av forordning (EF) nr. 767/2008, (EF) nr. 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU)
2018/1860, (EU) 2018/1861, (EU) 2019/817 og (EU) 2019/1896 fra Europaparlamentet og Rådet og om oppheving av rådsbeslutning 2004/512/EF og 2008/633/JHA, med det formål å reformere visuminformasjonssystemet (EUT L 248 av 13.7.2021, s. 11).

3. Eurodac

Europaparlaments- og rådsforordning (EU) 2024/1358 av 14. mai 2024 om av Eurodac for sammenligning av biometriske opplysninger for effektiv anvendelse av europaparlaments- og rådsforordning (EU) 2024/1315 og (EU) 2024/1350 og rådsdirektiv 2001/55/EF og for å identifisere tredjelandsborgere med ulovlig opphold og statsløse personer og om anmodninger om sammenligning med fra medlemsstatenes rettshåndhevelsesmyndigheter og Europol for rettshåndhevelsesformål, om endring av europaparlaments- og rådsforordning (EU) 2018/1240 og (EU 2019/818 og om oppheving av europaparlaments- og rådsforordning (EU) nr. 603/2013 (EUT L, 2024/1358 av 22.5.2024, ELI: http://data.europa. .eu/eli/reg/2024/1358/oj)

4. Inngangs-/utgangssystem

Europaparlaments- og rådsforordning (EU) 2017/2226 av 30. november 2017 om opprettelse av et inn- og utreisesystem (inn- og utreisesystemet) for registrering av inn- og utreiseopplysninger og opplysninger om nektet innreise for tredjelandsborgere som passerer medlemsstatenes ytre grenser, og om fastsettelse av vilkårene for tilgang til inn- og utreisesystemet for rettshåndhevelsesformål, og om endring av konvensjonen om gjennomføring av Schengen-avtalen og forordning (EF) nr. 767/2008 og (EU) nr. 1077/2011 (EUT L 327 av 9.12.2017, s. 20).

5. Europeisk system for reiseinformasjon og reisetillatelse

(a) Europaparlaments- og rådsforordning (EU) 2018/1240 av 12. september 2018 om opprettelse av et europeisk system for reiseinformasjon og reisetillatelse (ETIAS) og om endring av forordning (EU) nr. 1077/2011, (EU) nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 og (EU) 2017/2226 (EUT L 236 av 19.9.2018, s. 1).

(b) Europaparlaments- og rådsforordning (EU) 2018/1241 av 12. september 2018 om endring av forordning (EU) 2016/794 med det formål å opprette et europeisk system for reiseinformasjon og reisetillatelse (ETIAS) (EUT L 236 av 19.9.2018, s. 72).

6. Det europeiske strafferegisteret for tredjelandsborgere og statsløse personer

Europaparlaments- og rådsforordning (EU) 2019/816 av 17. april 2019 om opprettelse av et sentralisert system for identifisering av medlemsstater som har opplysninger om straffedommer mot tredjelandsborgere og statsløse personer (ECRIS-TCN) for å supplere det europeiske strafferegisterinformasjonssystemet og om endring av forordning (EU) 2018/1726 (EUT L 135 av 22.5.2019, s. 1).

7. Interoperabilitet

(a) Europaparlaments- og rådsforordning (EU) 2019/817 av 20. mai 2019 om fastsettelse av en ramme for interoperabilitet mellom EU-informasjonssystemer på grense- og visumområdet og om endring av forordning (EF) nr. 767/2008, (EU 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 og (EU) 2018/1861 av Europaparlamentet og Rådet og Rådets beslutninger 2004/512/EF og 2008/633/JHA (EUT L 135 av 22.5.2019, s. 27).

(b) Europaparlaments- og rådsforordning (EU) 2019/818 av 20. mai 2019 om etablering av en ramme for interoperabilitet mellom EU-informasjonssystemer på området politisamarbeid og rettslig samarbeid, asyl og migrasjon og om endring av forordning (EU) 2018/1726, (EU) 2018/1862 og (EU) 2019/816 (EUT L 135 av 22.5.2019, s. 85).

BILAG XI

Teknisk dokumentasjon nevnt i artikkel 53 nr. 1 bokstav a) - teknisk dokumentasjon for leverandører av generelle AI-modeller

Del 1

Informasjon som skal gis av alle leverandører av generelle aI-modeller

Den tekniske dokumentasjonen nevnt i artikkel 53 nr. 1 bokstav a) skal minst inneholde følgende opplysninger, avhengig av modellens størrelse og risikoprofil:

1. EN generell beskrivelse av den generelle aI-modellen, inkludert

   (a) hvilke oppgaver modellen er ment å utføre, og hvilken type og art KI-systemer den kan integreres i;

   (b) de gjeldende retningslinjene for akseptabel bruk;

   (c) dato for utgivelse og distribusjonsmetoder;

   (d) arkitekturen og antall parametere;

   (e) modalitet (f.eks. tekst, bilde) og format på inn- og utdata;

   (f) lisensen.

2. en detaljert beskrivelse av elementene i modellen nevnt i punkt 1, og relevant informasjon om prosessen for utviklingen, herunder følgende elementer

   (a) de tekniske virkemidlene (f.eks. bruksanvisninger, infrastruktur, verktøy) som kreves for at den generelle aI-modellen skal kunne integreres I aI-systemer;

   (b) spesifikasjonene for utformingen av modellen og opplæringsprosessen, inkludert opplæringsmetoder og -teknikker, de viktigste designvalgene, inkludert begrunnelser og antakelser, hva modellen er utformet for å optimalisere og relevansen av de ulike parameterne, der det er aktuelt;

   (c) informasjon om dataene som er brukt til opplæring, testing og validering, der det er relevant, inkludert type data og dataenes opprinnelse og kurateringsmetoder (f.eks. rensing, filtrering osv.), antall datapunkter, deres omfang og hovedkarakteristikker, hvordan dataene ble innhentet og valgt ut, samt alle andre tiltak for å oppdage uegnede datakilder og metoder for å oppdage identifiserbare skjevheter, der det er relevant;

   (d) beregningsressursene som brukes til å trene opp modellen (f.eks. antall flyttalloperasjoner), treningstid og andre relevante detaljer knyttet til treningen;

   (e) kjent eller estimert energiforbruk for modellen.

   Når det gjelder punkt (e), der modellens energiforbruk ukjent, kan energiforbruket baseres på informasjon om beregningsressurser som brukes.

Avsnitt 2

tilleggsinformasjon som skal gis av leverandører av generelle aI-modeller med systemrisiko

1. en detaljert beskrivelse av evalueringsstrategiene, inkludert evalueringsresultater, på grunnlag av tilgjengelige offentlige evalueringsprotokoller og -verktøy eller andre evalueringsmetoder. Evalueringsstrategiene skal omfatte evalueringskriterier, måleparametere og metodikk for identifisering av begrensninger.

2. Der det er relevant, en detaljert beskrivelse av tiltakene som er iverksatt for å gjennomføre interne og/eller eksterne kontradiktoriske tester (f.eks. red teaming), modelltilpasninger, inkludert justering og finjustering.

3. Der det er aktuelt, en detaljert beskrivelse av systemarkitekturen som forklarer hvordan programvarekomponentene bygger på hverandre og integreres i den samlede behandlingen.

BILAG XII

Åpenhetsinformasjon som nevnt i artikkel 53 nr. 1 bokstav b) - teknisk dokumentasjon for leverandører av generelle AI-modeller til nedstrømsleverandører som integrerer modellen i sitt AI-system

Opplysningene nevnt i artikkel 53 nr. 1 bokstav b) skal minst inneholde følgende

1. EN generell beskrivelse av den generelle aI-modellen, inkludert

   (a) hvilke oppgaver modellen er ment å utføre, og hvilken type og art KI-systemer den kan integreres i;

   (b) de gjeldende retningslinjene for akseptabel bruk;

   (c) dato for utgivelse og distribusjonsmetoder;

   (d) hvordan modellen samhandler, eller kan brukes til å samhandle, med maskinvare eller programvare som ikke er en del av selve modellen, der det er aktuelt;

   (e) versjonene av relevant programvare knyttet til bruk av den generelle aI-modellen, der det er aktuelt;

   (f) arkitekturen og antall parametere;

   (g) modalitet (f.eks. tekst, bilde) og format på inn- og utdata;

   (h) lisensen for modellen.

2. EN beskrivelse av elementene i modellen og av prosessen for utvikling av den, inkludert:

   (a) de tekniske hjelpemidlene (f.eks. bruksanvisninger, infrastruktur, verktøy) som kreves for at den generelle aI-modellen skal kunne integreres I aI-systemer;

   (b) modalitet (f.eks. tekst, bilde osv.) og formatet på inn- og utdataene og deres maksimale størrelse (f.eks. lengden på kontekstvinduet osv.);

   (c) informasjon om dataene som er brukt til opplæring, testing og validering, der det er aktuelt, inkludert type data, dataenes opprinnelse og kurateringsmetoder.

BILAG XIII

Kriterier for utpeking av generelle KI-modeller med systemrisiko som nevnt i artikkel 51

For å fastslå at en generell AI-modell har egenskaper eller en virkning som tilsvarer dem som er angitt i artikkel 51 nr. 1 bokstav a), skal Kommisjonen ta hensyn til følgende kriterier:

(a) antall parametere i modellen;

(b) kvaliteten eller størrelsen på datasettet, for eksempel målt gjennom tokens;

(c) Beregningsmengden som brukes til å trene opp modellen, målt i flyttalloperasjoner eller angitt ved en kombinasjon av andre variabler, for eksempel estimert kostnad for treningen, estimert tid som kreves for treningen eller estimert energiforbruk for treningen;

(d) modellens inngangs- og utgangsmodaliteter, f.eks. tekst til tekst (store språkmodeller), tekst til bilde, multimodalitet, og de nyeste terskelverdiene for å bestemme høy effekt for hver , og den spesifikke typen inndata og utdata (f.eks. biologiske sekvenser);

(e) referansene og evalueringene av modellens evner, blant annet med tanke på antall oppgaver uten ekstra opplæring, tilpasningsevne til å lære nye, distinkte oppgaver, graden av autonomi og skalerbarhet, og verktøyene den har tilgang til;

(f) om den har stor innvirkning på det indre marked på grunn av sin rekkevidde, noe som skal antas når den er gjort tilgjengelig for minst 10 000 registrerte bedriftsbrukere som er etablert i Unionen;

(g) antall registrerte sluttbrukere.