

EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2024/1689**av 13. juni 2024**

om fastsettelse av harmoniserte regler for 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 (forordningen om kunstig intelligens)

EUROPAPARLAMENTET OG RÅDET FOR DEN EUROPEISKE UNION HAR

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

under henvisning til forslag fra Europakommisjonen,

etter oversending av utkast til regelverksakt 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⁾,

etter den ordinære regelverksprosedyren⁽⁴⁾ og

ut fra følgende betraktninger:

- 1) Formålet med denne forordningen er å forbedre det indre markedes virkemåte ved å fastsette en ensartet rettslig ramme, særlig for utvikling, omsetning, utbredelse og bruk av systemer for kunstig intelligens (KI-systemer) i Unionen, i samsvar med Unionens verdier, for å fremme utbredelse av menneskesentrert og pålitelig kunstig intelligens (KI) samtidig som det sikres et høyt vernnivå for helse, sikkerhet og grunnleggende rettigheter som nedfelt i Den europeiske unions pakt om grunnleggende rettigheter («pakten»), herunder demokrati, rettsstatsprinsippet og miljøvern, for å beskytte mot de skadelige virkningene av KI-systemer i Unionen og for å støtte innovasjon. Denne forordningen sikrer fri bevegelighet over landegrensene for KI-baserte varer og tjenester, og hindrer dermed medlemsstatene i å legge restriksjoner på utvikling, markedsføring og bruk av KI-systemer med mindre denne forordningen uttrykkelig tillater dette.
- 2) Denne forordningen bør anvendes i samsvar med Unionens verdier slik de er nedfelt i pakten, og lette vernet av fysiske personer, foretak, demokratiet, rettsstatsprinsippet og miljøet, samtidig som den fremmer innovasjon og sysselsetting og gjør Unionen til en leder innen utbredelse av pålitelig KI.
- 3) KI-systemer kan lett settes i drift innenfor en lang rekke økonomiske sektorer og i mange deler av samfunnet, også på tvers av landegrensene, og kan lett spres i hele Unionen. Visse medlemsstater har allerede undersøkt muligheten for å vedta nasjonale regler for å sikre at KI er pålitelig og sikkert og utvikles og brukes i samsvar med forpliktelsene knyttet til grunnleggende rettigheter. Ulikheter mellom nasjonale regler kan føre til oppsplitting av det indre marked og svekke den rettslige forutsigbarheten for operatører som utvikler, importerer eller bruker KI-systemer. Det bør derfor sikres et konsekvent og høyt vernnivå i hele Unionen for å oppnå pålitelig KI, samtidig som forskjeller som hindrer fri omsetning, innovasjon, idriftsetting og utbredelse av KI-systemer og relaterte produkter og tjenester i det indre marked, bør forhindres ved å fastsette ensartede forpliktelser for operatørene og sikre et ensartet vern av tvingende allmenne hensyn og av personers rettigheter i hele det indre marked på grunnlag av artikkel 114 i traktaten om Den europeiske unions virkemåte (TEUV). I den utstrekning denne forordningen inneholder særlige regler om vern av fysiske personer i forbindelse med behandling av personopplysninger med hensyn til restriksjoner på bruk av KI-systemer til biometrisk

⁽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 rådsbeslutning av 21. mai 2024.

fjernidentifikasjon for rettshåndhevelsesformål, på bruk av KI-systemer til risikovurdering av fysiske personer for rettshåndhevelsesformål og på bruk av KI-systemer til biometrisk kategorisering for rettshåndhevelsesformål, bør denne forordningen, når det gjelder disse særlige reglene, baseres på artikkel 16 i TEUV. I lys av disse særlige reglene og anvendelsen av artikkel 16 i TEUV er det hensiktsmessig å rådføre seg med Det europeiske personvernråd.

- 4) KI er en familie av teknologier i rask utvikling som bidrar til et bredt spekter av økonomiske, miljømessige og samfunnsmessige fordeler over hele spekteret av bransjer og sosiale aktiviteter. Ved å forbedre prediksjon, optimalisere drift og ressurstildeling og persontilpasse digitale løsninger som er tilgjengelige for enkeltpersoner og organisasjoner, kan bruk av KI gi viktige konkurransefortrinn til foretak og bidra til sosialt og miljømessig gunstige resultater, for eksempel innen helse, landbruk, mattrygghet, utdanning og opplæring, medier, sport, kultur, infrastrukturforvaltning, energi, transport og logistikk, offentlige tjenester, sikkerhet, rettsvesen, ressurs- og energieffektivitet, miljøovervåking, bevaring og gjenoppretting av biologisk mangfold og økosystemer samt begrensning av og tilpasning til klimaendringer.
- 5) Samtidig kan KI, avhengig av omstendighetene rundt dens spesifikke anvendelse, bruk og grad av teknologisk utvikling, skape risiko og skade allmennhetens interesser og grunnleggende rettigheter som er beskyttet av unionsretten. Slik skade kan være materiell eller immateriell, herunder fysisk, psykisk, samfunnsmessig eller økonomisk skade.
- 6) I betraktning av den store innvirkningen KI kan ha på samfunnet, og behovet for å bygge tillit er det viktig at KI og regelverket for KI utvikles i samsvar med Unionens verdier som nedfelt i artikkel 2 i traktaten om Den europeiske union (TEU), de grunnleggende rettighetene og frihetene nedfelt i traktatene og, i medhold av artikkel 6 i TEU, paktene. Det bør være en forutsetning at KI er en menneskesentrert teknologi. Det bør fungere som et verktøy for mennesker og bør ha som endelig mål å øke menneskenes velferd.
- 7) For å sikre et ensartet og høyt vernnivå for allmennhetens interesser med hensyn til helse, sikkerhet og grunnleggende rettigheter bør det fastsettes felles regler for KI-systemer med høy risiko. Disse reglene bør være forenlige med paktene, 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 KI fra høynivågruppen for kunstig intelligens (AI HLEG).
- 8) Et unionsregelverk som fastsetter harmoniserte regler for KI, er derfor nødvendig for å fremme utvikling, bruk og utbredelse av KI i det indre marked, som samtidig sikrer et høyt vernnivå for allmennhetens interesser som helse og sikkerhet og vern av grunnleggende rettigheter, herunder demokrati, rettsstatsprinsippet og miljøvern, som anerkjent og beskyttet av unionsretten. For å nå dette målet bør det fastsettes regler for å bringe i omsetning, ta i bruk og bruke visse KI-systemer, slik at det sikres et velfungerende indre marked, og slik at disse systemene kan omfattes av prinsippet om fritt varebytte og fri bevegelse for tjenester. Disse reglene bør være klare og robuste når det gjelder å verne grunnleggende rettigheter, støtte nye innovative løsninger, muliggjøre et europeisk økosystem av offentlige og private aktører som skaper KI-systemer i tråd med Unionens verdier, og frigjøre potensialet i den digitale omstillingen i alle regioner i Unionen. Ved 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 en europeisk menneskesentrert tilnærming til kunstig intelligens og være en global leder i utviklingen av sikker, pålitelig og etisk KI, som uttalt av Det europeiske råd⁽⁵⁾, og den sikrer vern av etiske prinsipper, slik Europaparlamentet uttrykkelig har anmodet om⁽⁶⁾.

⁽⁵⁾ Det europeiske råd, Det europeiske råds ekstraordinære møte (1. og 2. oktober 2020) — Konklusjoner, EUCO 13/20, 2020, s. 6.

⁽⁶⁾ Europaparlamentsresolusjon av 20. oktober 2020 med anbefalinger til Kommisjonen om etiske aspekter ved kunstig intelligens, robotteknologi og beslektede teknologier, 2020/2012 (INL).

- 9) Harmoniserte regler for å bringe i omsetning, ta i bruk og bruke KI-systemer med høy risiko 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 som fastsettes i denne forordningen, bør gjelde på tvers av sektorer og bør i tråd med den nye rettslige rammen ikke berøre gjeldende unionsrett, særlig om vern av personopplysninger, forbrukervern, grunnleggende rettigheter, sysselsetting, vern av arbeidstakere og produktsikkerhet, som denne forordningen supplerer. Som følge av dette forblir alle rettigheter og rettsmidler som ved slik unionsrett gis til forbrukere og andre personer som KI-systemer kan ha en negativ innvirkning på, herunder med hensyn til erstatning for mulige skader i henhold til rådsdirektiv 85/374/EØF⁽¹⁰⁾, upåvirket og fullt ut gjeldende. Videre bør denne forordningen, når det gjelder sysselsetting og vern av arbeidstakere, derfor ikke berøre unionsretten om sosialpolitikk eller nasjonal arbeidsrett, i samsvar med unionsretten, om ansettelses- og arbeidsvilkår, herunder helse og sikkerhet på arbeidsplassen og forholdet mellom arbeidsgivere og arbeidstakere. Denne forordningen bør heller ikke berøre utøvelsen av de grunnleggende rettighetene som anerkjennes i medlemsstatene og på unionsplan, herunder retten eller friheten til å streike eller treffe andre tiltak som omfattes av de spesifikke arbeidsmarkedsordningene i medlemsstatene, eller retten til å forhandle fram, inngå og håndheve tariffavtaler eller treffe kollektive tiltak i samsvar med nasjonal rett. Denne forordningen bør ikke berøre de bestemmelsene med formål om å forbedre arbeidsvilkårene for plattformarbeidere som fastsettes i et europaparlaments- og rådsdirektiv om forbedring av arbeidsvilkårene for plattformarbeidere. Denne forordningen tar også sikte på å styrke effektiviteten til slike eksisterende rettigheter og rettsmidler ved å fastsette særlige krav og forpliktelser med hensyn til KI-systemer, herunder om åpenhet, teknisk dokumentasjon og registrering. Videre bør de forpliktelsene som pålegges ulike operatører i KI-verdikjeden i henhold til denne forordningen, gjelde uten at det berører nasjonal rett, i samsvar med unionsretten, som har den virkningen at bruken av visse KI-systemer begrenses dersom slik rett faller utenfor denne forordningens virkeområde eller forfølger andre legitime mål av allmenn interesse enn målene i denne forordningen. For eksempel bør denne forordningen ikke berøre nasjonale arbeidsrettsbestemmelser og bestemmelser om vern av mindreårige, det vil si personer under 18 år, idet det tas hensyn til FNs barnekonvensjons generelle kommentar nr. 25 (2021) om barns rettigheter i det digitale miljøet, med mindre de gjelder særskilt for KI-systemer og forfølger andre legitime mål av allmenn interesse.
- 10) Den grunnleggende retten til vern av personopplysninger sikres særlig ved europaparlaments- og rådsforordning (EU) 2016/679⁽¹¹⁾ og (EU) 2018/1725⁽¹²⁾ og europaparlaments- og rådsdirektiv (EU) 2016/680⁽¹³⁾. Europaparlaments- og rådsdirektiv 2002/58/EF⁽¹⁴⁾ verner i tillegg privatlivets fred og kommunikasjonsfortrolighet, blant annet ved å fastsette vilkår for all lagring av personopplysninger og ikke-personopplysninger i terminalutstyr og for tilgang til opplysningene fra terminalutstyr. Disse EU-rettsaktene danner grunnlaget for en bærekraftig og ansvarlig databehandling, herunder når datasettene omfatter en blanding av personopplysninger og ikke-personopplysninger. Denne forordningen søker ikke å påvirke anvendelsen av eksisterende unionsrett som regulerer behandling av personopplysninger, heller ikke oppgavene og fullmaktene til de uavhengige tilsynsmyndighetene som har kompetanse til å overvåke overholdelsen av disse instrumentene. Den berører heller ikke forpliktelsene til leverandører og idriftsettere av KI-systemer i deres rolle som behandlingsansvarlige eller databehandlere i henhold til unionsretten eller nasjonal rett om vern av personopplysninger, i den grad utformingen, utviklingen eller bruken av KI-systemer omfatter behandling av personopplysninger. Det bør også presiseres at de registrerte fortsatt har alle de rettighetene og garantiene som er gitt dem ved slik unionsrett, også rettighetene knyttet til utelukkende automatiserte individuelle avgjørelser, herunder profilering. Harmoniserte regler for å bringe i omsetning, ta i bruk og bruke KI-systemer som er fastsatt i samsvar med denne forordningen, bør lette en ef-
-
- (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 en felles ramme for markedsføring av produkter og om oppheving 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 produktsamsvar 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) Rådsdirektiv 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 samt om oppheving av direktiv 95/46/EF (generell personvernforordning) (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 samt 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 vedkommende myndigheters behandling av personopplysninger med henblikk på å forebygge, etterforske, avsløre eller straffeforfølge straffbare forhold eller iverksette strafferettslige sanksjoner, om fri utveksling av slike opplysninger og om oppheving av Rådets rammebeslutning 2008/977/JIS (EUT L 119 av 4.5.2016, s. 89).
- (14) Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon (direktivet om personvern og elektronisk kommunikasjon) (EFT L 201 av 31.7.2002, s. 37).

fektiv gjennomføring og gjøre det mulig for de registrerte å utøve sine rettigheter og andre rettsmidler som er garantert i henhold til unionsretten om vern av personopplysninger, samt andre grunnleggende rettigheter.

- 11) Denne forordningen bør ikke berøre bestemmelsene om ansvar for tilbydere av formidlingstjenester som fastsatt i europaparlaments- og rådsforordning (EU) 2022/2065⁽¹⁵⁾.
- 12) Begrepet «KI-system» i denne forordningen bør defineres klart og bør være nært tilpasset arbeidet til internasjonale organisasjoner som arbeider med KI, for å sikre rettslig forutsigbarhet, lette internasjonal tilnærming og bred aksept, samtidig som det gir fleksibilitet til å tilpasse seg den raske teknologiske utviklingen på dette området. Videre bør definisjonen baseres på sentrale kjennetegn ved KI-systemer som skiller dem fra enklere, tradisjonelle programvaresystemer eller programmeringsmetoder, og bør ikke omfatte systemer som er basert på regler som utelukkende er fastsatt av fysiske personer for å utføre operasjoner automatisk. Et sentralt kjennetegn ved KI-systemer er deres evne til å trekke slutninger. Med denne evnen til å trekke slutninger menes prosessen med å generere utdata, for eksempel prediksjoner, innhold, anbefalinger eller beslutninger, som kan påvirke fysiske og virtuelle miljøer, og KI-systemenes evne til å utlede modeller eller algoritmer, eller begge deler, fra data som mates inn i systemene, eller andre data. Blant de teknikkene som muliggjør utledning under oppbyggingen av et KI-system, er maskinlæringstilnærminger som på grunnlag av data lærer hvordan bestemte mål best kan nås, og logikk- og kunnskapsbaserte tilnærminger som trekker slutninger på grunnlag av kodet kunnskap eller symbolsk representasjon av oppgaven som skal løses. Et KI-systems evne til å trekke slutninger går lenger enn grunnleggende databehandling ved at det muliggjør læring, resonnering eller modellering. Begrepet «maskinbasert» viser til at KI-systemer kjøres på maskiner. Henvisningen til eksplisitte eller implisitte mål understreker at KI-systemer kan fungere i samsvar med uttrykkelige, definerte mål eller underforståtte mål. KI-systemets mål kan skille seg fra det tiltenkte formålet med KI-systemet i en bestemt sammenheng. I denne forordningen bør miljøer forstås som sammenhenger der KI-systemene opererer, mens resultater som genereres av KI-systemet, gjen-speiler ulike funksjoner som utføres av KI-systemer og omfatter prediksjoner, innhold, anbefalinger eller beslutninger. KI-systemer er utformet for å fungere med varierende grad av autonomi, noe som betyr at de til en viss grad er uavhengige av medvirkning fra mennesker og har evnen til å fungere uten menneskelig inngripen. Tilpasningsdyktigheten som et KI-system kan utvise etter at det er tatt i bruk, viser til selv læringsfunksjoner som gjør at systemet kan endre seg mens det er i bruk. KI-systemer kan brukes frittstående eller som en komponent i et produkt, uavhengig av om systemet er fysisk integrert i produktet (innebygd) eller tjener produktets funksjonalitet uten å være integrert i det (ikke-innebygd).
- 13) Begrepet «idriftsetter» i denne forordningen bør forstås som en fysisk eller juridisk person, herunder en offentlig myndighet, et byrå eller ethvert annet organ, som bruker et KI-system som er underlagt deres myndighet, unntatt når KI-systemet brukes i personlig, ikke-yrkesmessig virksomhet. Avhengig av typen KI-system kan bruken av systemet påvirke andre personer enn idriftsetteren.
- 14) Begrepet «biometriske opplysninger» brukt i denne forordningen bør tolkes i lys av begrepet slik det er 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 opplysninger kan gjøre det mulig å autentisere, identifisere eller kategorisere fysiske personer og gjenkjenne fysiske personers følelser.
- 15) Begrepet «biometrisk identifikasjon» i denne forordningen bør defineres som automatisk gjenkjenning av fysiske, fysiologiske og atferdsmessige menneskelige egenskaper som ansikt, øyebevegelser, kroppsform, stemme, prosodi, gange, holdning, hjerterefrekvens, blodtrykk, lukt og kjennetegn ved tastetrykk, med det formålet å fastslå en persons identitet ved å sammenligne den personens biometriske opplysninger med lagrede biometriske opplysninger om personer i en referansedatabase, uavhengig av om personen har gitt sitt samtykke eller ikke. Dette utelukker KI-systemer som er ment å brukes til biometrisk verifisering, som inkluderer autentisering, og hvis eneste formål er å bekrefte at en bestemt fysisk person er den som han eller hun utgir seg for å være, og å bekrefte identiteten til en fysisk person med det eneste formålet å få tilgang til en tjeneste, låse opp en enhet eller få sikkerhetsadgang 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 (forordningen om digitale tjenester) (EUT L 277 av 27.10.2022, s. 1).

- 16) Begrepet «biometrisk kategorisering» i denne forordningen bør defineres som å plassere fysiske personer i bestemte kategorier på grunnlag av deres biometriske opplysninger. Slike kategorier kan ha sammenheng med kjennetegn som kjønn, alder, hårfarge, øyenfarge, tatoveringer, atferds- eller personlighetstrekk, språk, religion, tilhørighet til en nasjonal minoritet, seksuell legning eller politisk ståsted. Dette inkluderer ikke biometriske kategoriseringssystemer som er en rent underordnet funksjon uløselig knyttet til en annen kommersiell tjeneste, noe som innebærer at funksjonen av objektive tekniske årsaker ikke kan brukes uten hovedtjenesten, og at integreringen av denne funksjonen eller funksjonaliteten ikke er et middel til å omgå anvendelsen av reglene i denne forordningen. For eksempel kan filtre som brukes på nettbaserte markeds plasser for å kategorisere ansiktstrekk eller kroppslige trekk, utgjøre en slik tilleggsfunksjon, ettersom de bare kan brukes i sammenheng med hovedtjenesten, som er å selge et produkt, ved å gi forbrukeren mulighet til på forhånd å se hvordan produktet vil ta seg ut på ham eller henne, og hjelpe vedkommende å treffe en kjøpsbeslutning. Filtre som brukes på sosiale nettverkstjenester på internett, og som kategoriserer ansiktstrekk eller kroppslige trekk for at brukerne skal kunne legge til eller endre bilder eller videoer, kan også anses å være en tilleggsfunksjon, ettersom et slikt filter ikke kan brukes uten hovedtjenesten, som er deling av innhold på internett.
- 17) Begrepet «system for biometrisk fjernidentifikasjon» i denne forordningen bør defineres funksjonelt, som et KI-system som er beregnet på å identifisere fysiske personer uten deres aktive medvirkning, vanligvis på avstand, ved å sammenligne en persons biometriske opplysninger med de biometriske opplysningene i en referansedatabase, uavhengig av teknologien, prosessene eller typen biometriske opplysninger som brukes. Slike systemer for biometrisk fjernidentifikasjon brukes vanligvis for å oppfatte flere personer eller deres atferd samtidig, for vesentlig å lette identifikasjonen av fysiske personer uten deres aktive medvirkning. Dette utelukker KI-systemer som er ment å brukes til biometrisk verifisering, som inkluderer autentisering, og hvis eneste formål er å bekrefte at en bestemt fysisk person er den som han eller hun utgir seg for å være, og å bekrefte identiteten til en fysisk person med det eneste formålet å få tilgang til en tjeneste, låse opp en enhet eller få sikkerhetsadgang til lokaler. Dette unntaket er begrunnet med at slike systemer forventes å ha liten innvirkning på fysiske personers grunnleggende rettigheter sammenlignet med de systemene for biometrisk fjernidentifikasjon som kan brukes til å behandle de biometriske opplysningene til et stort antall personer uten deres aktive medvirkning. Når det gjelder sanntidssystemer, skjer registreringen av de biometriske opplysningene, sammenligningen og identifikasjonen øyeblikkelig, nesten øyeblikkelig eller under alle omstendigheter uten vesentlig forsinkelse. I denne forbindelsen bør det ikke være rom for å omgå denne forordningens regler om sanntidsbruk av de aktuelle KI-systemene ved å legge inn mindre forsinkelser. Sanntidssystemer innebærer bruk av materiale som vises direkte eller nesten direkte, for eksempel videobilder, og som genereres av et kamera eller en annen enhet med lignende funksjonalitet. Når det gjelder ettertidssystemer, derimot, har de biometriske opplysningene allerede blitt registrert, og sammenligningen og identifikasjonen skjer først vesentlig senere. Dette omfatter materiale, for eksempel bilder eller video fra overvåkingskameraer eller private enheter, som har blitt generert før systemet brukes på de berørte fysiske personene.
- 18) Begrepet «følelsesgjenkjenningssystem» i denne forordningen bør defineres som et KI-system som har som formål å identifisere eller utlede fysiske personers følelser eller intensjoner på grunnlag av deres biometriske opplysninger. Begrepet viser til følelser eller intensjoner som glede, bedrøvelse, sinne, overraskelse, avsky, forlegenhet, opphisselse, skam, forakt, tilfredshet og fornøyelse. Det omfatter ikke fysiske tilstander, for eksempel smerte eller tretthet, heller ikke for eksempel systemer som brukes til å registrere tretthet hos yrkesflygere eller -førere med henblikk på å hindre ulykker. Det omfatter heller ikke ren registrering av lett synlige uttrykk, fakter eller bevegelser, med mindre de brukes til å identifisere eller utlede følelser. Dette kan være vanlige ansiktsuttrykk, for eksempel en rynket panne eller et smil, eller fakter som å bevege hendene, armene eller hodet, eller kjennetegn ved en persons stemme, for eksempel hevet stemme eller hvisking.
- 19) I denne forordningen bør begrepet «offentlig tilgjengelig sted» forstås som ethvert fysisk sted som er tilgjengelig for et ubestemt antall fysiske personer, uansett om det aktuelle stedet er privat eller offentlig eid, og uansett hvilke aktiviteter stedet kan brukes til, så som handel, for eksempel butikker, restauranter eller kafeer – tjenester, for eksempel banker, yrkesvirksomhet eller overnattingssteder – idrett, for eksempel svømmebasseng, treningssentre eller stadioner – transport, for eksempel buss-, metro- og jernbanestasjoner, lufthavner eller transportmidler – underholdning, for eksempel kinoer, teatre, museer eller konsert- og konferansesaler – eller fritidsaktiviteter og annen bruk, for eksempel offentlige veier og torg, parker, skoger eller lekeplasser. Et sted bør også regnes som offentlig tilgjengelig dersom, uavhengig av potensiell kapasitet eller sikkerhetsrestriksjoner, adgangen til stedet er underlagt visse forhåndsbestemte vilkår som kan oppfylles av et ubestemt antall personer, for eksempel kjøp av billett eller reisebevis, forhåndsregistrering eller å ha nådd en viss alder. Derimot bør et sted ikke anses som offentlig tilgjengelig dersom adgangen er forbeholdt bestemte og definerte fysiske personer ved enten unionsrett eller nasjonal rett som er direkte knyttet til offentlig sikkerhet, eller ved at personen som har den relevante myndigheten over stedet, tydelig uttrykker sin vilje. Utelukkende det faktum at det er mulig å få adgang, for eksempel en ulåst dør eller en åpen port i et gjerde, innebærer ikke at stedet er offentlig tilgjengelig dersom det er indikasjoner eller omstendigheter til stede som tyder på det motsatte, for eksempel skilt som forbyr eller begrenser adgangen. Foretaks- og fabrikklokaler og kontorer og arbeidsplasser som bare relevante ansatte og tjenesteytere er ment å ha adgang til, er ikke offentlig tilgjengelige steder. Offentlig tilgjengelige steder bør

ikke omfatte fengsler eller grensekontrollsteder. Enkelte andre steder kan omfatte både offentlig tilgjengelige og ikke offentlig tilgjengelige områder, for eksempel entreen til et privat boligbygg som er nødvendig for å få adgang til et legekontor, eller hallene i en lufthavn. Nettsteder er ikke dekket, ettersom de ikke er fysiske steder. Hvorvidt et gitt sted er tilgjengelig for offentligheten, bør imidlertid avgjøres i hvert enkelt tilfelle, ut fra de særlige omstendighetene.

- 20) For å få størst mulig nytte av KI-systemer, samtidig som grunnleggende rettigheter, helse og sikkerhet vernes, og for å gi mulighet for demokratisk kontroll bør KI-kompetanse gi leverandører, idriftsettere og berørte personer de begrepene som er nødvendige for å treffe informerte beslutninger om KI-systemer. Disse begrepene kan variere avhengig av den relevante sammenhengen og kan innebære å forstå korrekt bruk av tekniske elementer under KI-systemets utviklingsfase, tiltakene som skal anvendes under bruken av KI-systemet, passende måter å tolke KI-systemets utdata på, og, når det gjelder berørte personer, den kunnskapen som er nødvendig for å forstå hvordan beslutninger som treffes med hjelp fra KI, vil påvirke dem. I sammenheng med anvendelsen av denne forordningen bør KI-kompetanse gi alle relevante aktører i KI-verdikjeden den innsikten som kreves for å sikre overholdelse og korrekt håndhevelse av forordningen. Dessuten kan utstrakt gjennomføring av tiltak for å gi KI-kompetanse og innføring av egnede oppfølgingstiltak bidra til å bedre arbeidsvilkårene og i siste instans opprettholde konsolideringen av og innovasjonsbanen for pålitelig KI i Unionen. Det europeiske rådet for kunstig intelligens («KI-rådet») bør støtte Kommisjonen i å fremme verktøy for KI-kompetanse, og allmennhetens kjennskap til og forståelse av fordeler, risikoer, sikkerhetstiltak, rettigheter og forpliktelser ved bruk av KI-systemer. I samarbeid med de relevante berørte partene bør Kommisjonen og medlemsstatene legge til rette for at det utarbeides frivillige atferdsregler for å fremme KI-kompetanse blant personer som arbeider med utvikling, drift og bruk av KI.
- 21) For å sikre like konkurransevilkår og effektivt vern av enkeltpersoners rettigheter og friheter i hele Unionen bør reglene som fastsettes ved denne forordningen, få anvendelse på leverandører av KI-systemer på en ikke-diskriminerende måte, uansett om de er etablert i Unionen eller i et tredjeland, og på idriftsettere av KI-systemer som er etablert i Unionen.
- 22) På grunn av sin digitale natur bør visse KI-systemer omfattes av denne forordningens virkeområde selv når de ikke bringes i omsetning, tas i bruk eller brukes i Unionen. Dette er for eksempel tilfellet når en operatør etablert i Unionen setter ut visse tjenester på kontrakt til en operatør etablert i et tredjeland i forbindelse med en aktivitet som skal utføres av et KI-system som er å anse som et KI-system med høy risiko. Under disse omstendighetene kan det KI-systemet som brukes av operatøren i tredjelandet, behandle data som er lovlig innsamlet i og overført fra Unionen, og gi den kontraherende operatøren i Unionen utdataene fra nevnte KI-system som genereres ved denne behandlingen, uten at dette KI-systemet bringes i omsetning, tas i bruk eller brukes i Unionen. For å hindre omgåelse av denne forordningen og sikre et effektivt vern av fysiske personer i Unionen bør denne forordningen også få anvendelse på leverandører og idriftsettere av KI-systemer som er etablert i et tredjeland, i den utstrekning utdataene fra disse systemene er beregnet på å brukes i Unionen. For å ta hensyn til eksisterende ordninger og særlige behov for framtidig samarbeid med utenlandske partnere som det utveksles informasjon og bevis med, bør denne forordningen likevel ikke få anvendelse på et tredjlands offentlige myndigheter eller på internasjonale organisasjoner når de opptrer innenfor rammen av samarbeid eller internasjonale avtaler som er inngått på unionsplan eller nasjonalt plan om rettshåndhevelse og rettslig samarbeid med Unionen eller medlemsstatene, forutsatt at det relevante tredjelandet eller den relevante internasjonale organisasjonen gir tilstrekkelige garantier med hensyn til vern av fysiske personers grunnleggende rettigheter og friheter. Når det er relevant, kan dette omfatte virksomhet som utøves av enheter som er gitt i oppdrag av tredjeland å utføre bestemte oppgaver til støtte for slik rettshåndhevelse og slikt rettslig samarbeid. Slike samarbeidsrammer eller avtaler er fastsatt bilateralt mellom medlemsstater og tredjeland eller mellom Den europeiske union, Europol og andre EU-organer på den ene siden, og tredjeland og internasjonale organisasjoner på den andre. Myndighetene med ansvar for å føre tilsyn med de rettshåndhevende myndighetene og rettsmyndighetene i samsvar med denne forordningen bør vurdere om disse samarbeidsrammene eller internasjonale avtalene gir tilstrekkelige garantier med hensyn til vern av fysiske personers grunnleggende rettigheter og friheter. Mottakende nasjonale myndigheter og Unionens institusjoner, organer, kontorer og byråer som gjør bruk av slike utdata i Unionen, er ansvarlige for å sikre at bruken er i samsvar med unionsretten. Når disse internasjonale avtalene revideres eller nye inngås i framtiden, bør avtalepartene gjøre sitt ytterste for å bringe disse avtalene i samsvar med kravene i denne forordningen.

- 23) Denne forordningen bør også få anvendelse på Unionens institusjoner, organer, kontorer og byråer når de opptrer som leverandør eller idriftsetter av et KI-system.
- 24) Dersom og i den grad KI-systemer bringes i omsetning, tas i bruk eller brukes med eller uten endringer for militære formål, forsvarsformål eller formål knyttet til nasjonal sikkerhet, bør disse utelukkes fra denne forordningens virkeområde uansett hvilken type enhet som utfører disse aktivitetene, for eksempel om det er en offentlig eller privat enhet. Når det gjelder militære formål og forsvarsformål, begrunnes en slik utelukkelse både av artikkel 4 nr. 2 i TEU og særtrekene ved medlemsstatenes og Unionens felles forsvarspolitik, som omfattes av avdeling V kapittel 2 i TEU og er underlagt folkeretten, som derfor er den mest hensiktsmessige 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, begrunnes utelukkelsen både av det faktum at nasjonal sikkerhet er medlemsstatenes eneansvar i samsvar med artikkel 4 nr. 2 i TEU, og av den nasjonale sikkerhetsvirksomhetens særlige karakter og operasjonelle behov samt de særlige nasjonale reglene som gjelder for denne virksomheten. Ikke desto mindre vil et KI-system som er utviklet, er brakt i omsetning, er tatt i bruk eller brukes for militære formål, forsvarsformål eller formål knyttet til nasjonal sikkerhet, falle inn under denne forordningens virkeområde dersom det midlertidig eller permanent brukes for andre formål, for eksempel sivile eller humanitære formål, rettsåndhevelsesformål eller formål knyttet til offentlig sikkerhet. I så fall bør den enheten som bruker KI-systemet for andre formål enn militære formål, forsvarsformål eller formål knyttet til nasjonal sikkerhet, sikre at KI-systemet er i samsvar med denne forordningen, med mindre systemet allerede er i samsvar med denne forordningen. KI-systemer som bringes i omsetning eller tas i bruk for et utelukket formål, det vil si for et militært formål, forsvarsformål eller et formål knyttet til nasjonal sikkerhet, og for ett eller flere ikke-utelukkede formål, for eksempel sivile formål eller rettsåndhevelsesformål, faller innenfor denne forordningens virkeområde, og leverandører av disse systemene bør sikre overholdelse av denne forordningen. I disse tilfellene bør det faktum at et KI-system kan falle inn under denne forordningens virkeområde, ikke være til hinder for at enheter som utfører nasjonale sikkerhetsaktiviteter, forsvarsaktiviteter og militære aktiviteter, uansett hvilken type enhet som utfører disse aktivitetene, kan bruke KI-systemer for formål knyttet til nasjonal sikkerhet, for militære formål og for forsvarsformål, ettersom slik bruk er utelukket fra denne forordningens virkeområde. Et KI-system som bringes i omsetning for sivile formål eller rettsåndhevelsesformål, og som brukes med eller uten endringer for militære formål, forsvarsformål eller formål knyttet til nasjonal sikkerhet, bør ikke omfattes av denne forordningens virkeområde, uansett hvilken type enhet som utfører disse aktivitetene.
- 25) Denne forordningen bør støtte innovasjon, respektere vitenskapens frihet og ikke undergrave forsknings- og utviklingsaktivitet. Derfor må KI-systemer og -modeller som er spesialutviklet og tatt i bruk utelukkende med henblikk på vitenskapelig forskning og utvikling, utelukkes fra forordningens virkeområde. Det er videre nødvendig å sikre at denne forordningen ikke på annen måte påvirker vitenskapelig forskning på og utvikling av KI-systemer eller -modeller før de bringes i omsetning eller tas i bruk. Når det gjelder produktorientert forsknings-, test- og utviklingsaktivitet med hensyn til KI-systemer eller -modeller, bør bestemmelsene i denne forordningen heller ikke få anvendelse før disse systemene og modellene tas i bruk eller bringes i omsetning. Dette unntaket berører ikke forpliktelsen til å overholde denne forordningen dersom et KI-system som faller innenfor dens virkeområde, bringes i omsetning eller tas i bruk som følge av slik forsknings- og utviklingsaktivitet, og berører heller ikke anvendelsen av bestemmelser om regulatoriske sandkasser for KI og testing under virkelige forhold. Dessuten, uten at det berører utelukkelsen av KI-systemer som er spesialutviklet og tatt i bruk utelukkende med henblikk på vitenskapelig forskning og utvikling, bør ethvert annet KI-system som kan brukes til gjennomføring av forsknings- og utviklingsaktiviteter, fortsatt være underlagt bestemmelsene i denne forordningen. Under alle omstendigheter bør alle forsknings- og utviklingsaktiviteter utføres i samsvar med anerkjente etiske og faglige standarder for vitenskapelig forskning og i samsvar med gjeldende unionsrett.
- 26) For å innføre et forholdsmessig og effektivt sett med bindende regler for KI-systemer bør det følges en klart definert risikobasert tilnærming. I denne tilnærmingen bør typen av og innholdet i slike regler tilpasses styrken og omfanget av de risikoene som KI-systemer kan skape. Det er derfor nødvendig å forby visse former for uakseptabel KI-praksis, å fastsette krav til KI-systemer med høy risiko og forpliktelser for de relevante operatørene, og å fastsette forpliktelser om åpenhet med hensyn til visse KI-systemer.

- 27) Selv om den risikobaserte tilnærmingen er grunnlaget for et forholdsmessig og effektivt sett med bindende regler, er det viktig å minne om de etiske retningslinjene for pålitelig KI fra 2019, som er utarbeidet av den uavhengige høynivågruppen for kunstig intelligens utnevnt av Kommisjonen (AI HLEG). I disse retningslinjene har AI HLEG utviklet sju ikke-bindende etiske prinsipper for KI som skal bidra til å sikre at KI er pålitelig og etisk forsvarlig. De sju prinsippene omfatter menneskelig handlekraft og tilsyn, teknisk robusthet og sikkerhet, personvern og dataforvaltning, åpenhet, mangfold, ikke-diskriminering og rettferdighet samt samfunnsmessig og miljømessig velferd og ansvarlighet. Uten at det berører de rettslig bindende kravene i denne forordningen og annen gjeldende unionsrett, bidrar disse retningslinjene til utforming av sammenhengende, pålitelig og menneskesentrert KI, i samsvar med pakten og de verdiene som Unionen bygger på. Ifølge retningslinjene fra AI HLEG betyr menneskelig organisering og tilsyn at KI-systemer utvikles og brukes som et verktøy som tjener mennesker, respekterer menneskelig verdighet og personlig autonomi, og som fungerer slik at de på en egnet vis kan kontrolleres og overvåkes av mennesker. Teknisk robusthet og sikkerhet betyr at KI-systemer utvikles og brukes på en måte som muliggjør robusthet i tilfelle av problemer samt motstandsdyktighet mot forsøk på å endre bruken av eller ytelsen til KI-systemet i den hensikt å gi mulighet for ulovlig bruk fra tredjeparter, og som minimerer utilsiktet skade. Personvern og dataforvaltning betyr at KI-systemer utvikles og brukes i samsvar med regler for personvern og vern av personopplysninger, samtidig som databehandlingen oppfyller høye standarder for kvalitet og integritet. Åpenhet betyr at KI-systemer utvikles og brukes på en måte som muliggjør tilfredsstillende sporbarhet og forklarbarhet, samtidig som mennesker gjøres oppmerksomme på at de kommuniserer eller samhandler med et KI-system, samt at idriftsettere blir behørig informert om KI-systemets kapasitet og begrensninger og berørte personer om sine rettigheter. Mangfold, ikke-diskriminering og rettferdighet betyr at KI-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 urimelige skjevheter som er forbudt i henhold til unionsretten eller nasjonal rett. Sosial og miljømessig velferd betyr at KI-systemer utvikles og brukes på en bærekraftig og miljøvennlig måte som kommer alle mennesker til gode, samtidig som de langsiktige konsekvensene for individet, samfunnet og demokratiet overvåkes og vurderes. Anvendelsen av disse prinsippene bør om mulig omsettes i utformingen og bruken av KI-modeller. De bør under alle omstendigheter tjene som grunnlag for utarbeiding av atferdsregler i henhold til denne forordningen. Alle berørte parter, herunder næringsliv, academia, sivilsamfunnet og standardiseringsorganisasjoner, oppfordres til å ta hensyn til de etiske prinsippene for utvikling av frivillig beste praksis og standarder.
- 28) Ved siden av at KI kan brukes til mye nyttig, kan det også misbrukes og gi opphav til nye og kraftige verktøy for manipulering, utnyttning og sosial kontroll. Slik praksis er særlig skadelig og krenkende og bør forbys fordi den strider mot Unionens verdier om respekt for menneskets verdighet, frihet, likhet, demokrati og rettsstatsprinsippet samt de grunnleggende rettighetene som er nedfelt i pakten, herunder retten til ikke-diskriminering, vern av personopplysninger, personvern og barns rettigheter.
- 29) KI-baserte manipulative teknikker kan brukes til å overtale personer til å oppføre seg på en uønsket måte eller til å villede dem ved å oppmuntre dem til å treffe beslutninger på en måte som undergraver og svekker deres selvstendighet, beslutningstaking og frie valg. Å bringe i omsetning, ta i bruk eller bruke visse KI-systemer med det formålet eller den virkningen at menneskelig atferd endres vesentlig, og som kan forventes å forårsake betydelig skade, særlig med tilstrekkelig stor negativ innvirkning på fysisk eller psykisk helse eller økonomiske interesser, er særlig farlig og bør derfor forbys. Slike KI-systemer bruker subliminale komponenter som lyd-, bilde- eller videostimuli som mennesker ikke kan oppfatte, ettersom de ligger utenfor den menneskelige oppfatningsevnen, eller andre manipulative eller villedende teknikker som undergraver eller svekker menneskers selvstendighet, beslutningstaking eller frie valg på slike måter at mennesker ikke er bevisst oppmerksomme på disse teknikkene, eller selv om de er oppmerksomme på dem, likevel kan bli villedet eller ikke er i stand til å kontrollere eller motstå dem. Dette kan lettes for eksempel ved bruk av maskin-hjerne-grensesnitt eller virtuell virkelighet, ettersom dette gir mulighet for større grad av kontroll over hvilke stimuli som presenteres for personer, i den grad at de vesentlig kan endre personenes atferd på en måte som forårsaker betydelig skade. KI-systemer kan også på annen måte utnytte sårbarhetene hos en person eller en bestemt gruppe personer på bakgrunn av alder, nedsatt funksjonsevne som definert i europaparlaments- og rådsdirektiv (EU) 2019/882⁽¹⁶⁾ eller en bestemt sosial eller økonomisk situasjon som kan forventes å gjøre disse personene mer sårbare for utnyttning, for eksempel personer som lever i ekstrem fattigdom, eller etniske eller religiøse minoriteter. Slike KI-systemer kan bringes i omsetning, tas i bruk eller brukes med det formålet eller den virkningen at atferden til en person endres vesentlig og på en måte som påfører eller med rimelighet kan forventes å påføre denne personen eller en annen person eller grupper av personer betydelig skade, herunder skade som kan akkumuleres over tid, og bør derfor forbys. Det kan ikke nødvendigvis forutsettes at det foreligger en hensikt om å endre atferd, dersom atferdsendringen skyldes faktorer utenfor KI-systemet og utenfor leverandørens eller idriftsetterens kontroll, det vil si faktorer som det ikke nødvendigvis er rimelig å forutse, og som det derfor ikke er mulig for leverandøren eller idriftsetteren av KI-systemet å avbøte. I alle tilfeller kre-

⁽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).

ves det ikke at leverandøren eller idriftsetteren har til hensikt å forårsake betydelig skade, forutsatt at skaden skyldes manipulativ eller utnyttende KI-basert praksis. Forbudene mot slik KI-praksis kommer i tillegg til bestemmelsene i europaparlaments- og rådsdirektiv 2005/29/EF⁽¹⁷⁾, særlig at urimelig handelspraksis som fører til økonomisk eller finansiell skade for forbrukerne, er forbudt under alle omstendigheter, uansett om den iverksettes ved hjelp av KI-systemer eller på annen måte. Forbudene mot manipulativ og utnyttende praksis i denne forordningen bør ikke berøre lovlig praksis i forbindelse med medisinsk behandling, for eksempel psykologisk behandling av en psykisk sykdom eller fysisk rehabilitering, når slik praksis utføres i samsvar med gjeldende rett og medisinske standarder, for eksempel uttrykkelig samtykke fra enkeltpersonene eller deres juridiske representanter. Dessuten bør vanlig og legitim handelspraksis, for eksempel på reklameområdet, som er i samsvar med gjeldende rett, ikke i seg selv anses å utgjøre skadelig manipulativ KI-basert praksis.

- 30) Biometriske kategoriseringssystemer som er basert på fysiske personers biometriske opplysninger, for eksempel en persons ansikt eller fingeravtrykk, for å utlede en persons politiske meninger, fagforeningsmedlemskap, religiøse eller filosofiske overbevisning, rase, seksuell liv eller seksuelle legning, bør forbys. Dette forbudet bør ikke omfatte at biometriske datasett som er innhentet i samsvar med unionsretten eller nasjonal rett, merkes, filtreres eller kategoriseres basert på biometriske opplysninger, for eksempel sortering av bilder etter hårfarge eller øyenfarge, som for eksempel kan forekomme på rettshåndhevelsesområdet.
- 31) KI-systemer som gir offentlige eller private aktører mulighet til sosial rangering av fysiske personer, kan få diskriminerende utfall og føre til utestenging av visse grupper. De kan krenke retten til verdighet og ikke-diskriminering og verdiene likhet og rettferdighet. Slike KI-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, utledede eller forutsagte personlige egenskaper eller personlighetstrekk over bestemte tidsperioder. Den sosiale rangeringen som oppnås med slike KI-systemer, kan føre til skadelig eller ugunstig behandling av fysiske personer eller hele grupper av fysiske personer i sosiale sammenhenger som ikke er relatert til den sammenhengen der dataene opprinnelig ble generert eller innhentet, eller til skadelig behandling som ikke står i forhold til eller er urettmessig ut fra alvorlighetsgraden av den sosiale atferden deres. KI-systemer som medfører slik uakseptabel rangeringspraksis og får slike skadelige eller ugunstige utfall, bør derfor forbys. Dette forbudet bør ikke berøre lovlige former for evaluering av fysiske personer som utføres for et bestemt formål i samsvar med unionsretten og nasjonal rett.
- 32) Bruk av KI-systemer til biometrisk fjernidentifikasjon av fysiske personer i sanntid på offentlig tilgjengelige steder med henblikk på rettshåndhevelse griper særlig inn i rettighetene og frihetene til de berørte personene, i en slik grad at det kan påvirke privatlivet til en stor del av befolkningen, gi en følelse av konstant overvåking og indirekte avskrekke folk fra å utøve forsamlingsfriheten og andre grunnleggende rettigheter. Tekniske unøyaktigheter i KI-systemer som er beregnet på biometrisk fjernidentifikasjon av fysiske personer, kan gi skjeve resultater og diskriminerende virkninger. Slike mulige skjeve resultater og diskriminerende virkninger er særlig relevante når det gjelder alder, etnisitet, rase, kjønn eller funksjonsnedsettelse. Den umiddelbare innvirkningen og de begrensede mulighetene for ytterligere kontroll eller rettelser i forbindelse med bruken av slike sanntidssystemer medfører dessuten økt risiko for de berørte personenes rettigheter og friheter i forbindelse med, eller som påvirkes av, rettshåndhevelsesaktiviteter.
- 33) Bruk av disse systemene for rettshåndhevelsesformål bør derfor forbys, unntatt i situasjoner som er oppført på en uttømmende liste og snevert definert, der bruken er strengt nødvendig for å oppnå en viktig allmenn interesse med en betydning som veier tyngre enn risikoene. Disse situasjonene omfatter søk etter visse ofre for kriminalitet, herunder savnede personer, visse trusler mot fysiske personers liv eller fysiske sikkerhet eller om et terrorangrep, og lokalisering eller identifikasjon av personer som har begått eller er mistenkt for å ha begått de straffbare handlingene som er oppført i et vedlegg til denne forordningen, når disse straffbare handlingene i medlemsstaten det gjelder, kan straffes med frihetsstraff eller et annet frihetsberøvende tiltak med maksimal soningstid på minst fire år, og slik de er definert i denne medlemsstatens rett. En slik terskel for frihetsstraffen eller det frihetsberøvende tiltaket i samsvar med nasjonal rett bidrar til å sikre at overtredelsen er tilstrekkelig alvorlig til at den potensielt rettferdiggjør bruk av systemer for biometrisk fjernidentifikasjon i sanntid. Dessuten er listen over straffbare handlinger oppført i et vedlegg til denne forordningen basert på de 32 straffbare handlingene som er listet opp i Rådets rammebeslutning 2002/584/JIS⁽¹⁸⁾, samtidig som det er tatt hensyn til at noen av disse straffbare handlingene i praksis trolig vil være mer relevante enn andre, ved at det vil va-

⁽¹⁷⁾ Europaparlaments- og rådsdirektiv 2005/29/EF av 11. mai 2005 om foretaks urimelige handelspraksis overfor forbrukere på 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 europaparlaments- og rådsforordning (EF) nr. 2006/2004 (direktivet om urimelig handelspraksis) (EUT L 149 av 11.6.2005, s. 22).

⁽¹⁸⁾ Rådets rammebeslutning 2002/584/JIS av 13. juni 2002 om den europeiske arrestordre og prosedyrene for overlevering mellom medlemsstatene (EFT L 190 av 18.7.2002, s. 1).

riere mye hvor nødvendig og forholdsmessig det er å bruke biometrisk fjernidentifikasjon i sanntid i det praktiske arbeidet med å lokalisere eller identifisere en person som har eller er mistenkt for å ha begått de forskjellige straffbare handlingene på listen, og tatt i betraktning de sannsynlige forskjellene i skadens eller de mulige negative konsekvensenes alvorlighetsgrad, sannsynlighet og omfang. En overhengende trussel mot fysiske personers liv eller fysiske sikkerhet kan også oppstå som 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 grunnleggende forsyninger til befolkningen eller utøvelsen av statens kjernefunksjon. I tillegg bør denne forordningen bevare muligheten for rettshåndhevende myndigheter, grensekontroll-, innvandrings- eller asylmyndigheter til å foreta identitetskontroller i nærvær av den berørte personen i samsvar med vilkårene fastsatt i unionsretten og nasjonal rett om slike kontroller. Særlig bør rettshåndhevende myndigheter, grensekontroll-, innvandrings- eller asylmyndigheter kunne bruke informasjonssystemer i samsvar med unionsretten eller nasjonal rett til å identifisere personer som under en identitetskontroll enten nekter å bli identifisert eller ikke er i stand til å oppgi eller bevise sin identitet, uten å være pålagt ved denne forordningen å innhente forhåndstillatelse. Dette kan for eksempel være en person som er involvert i en forbrytelse, og som er uvillig til eller på grunn av en ulykke eller medisinsk tilstand er ute av stand til å avsløre sin identitet til rettshåndhevende myndigheter.

- 34) For å sikre at disse systemene brukes på en ansvarlig og forholdsmessig måte, er det også viktig å fastsette at det i hver av disse uttømmende opplistede og snevert definerte situasjonene bør tas hensyn til visse faktorer, særlig når det gjelder karakteren av den situasjonen som gir opphav til anmodningen, og de konsekvensene som bruken har for rettighetene og frihetene til alle berørte personer, samt de sikkerhetstiltakene og vilkårene som er fastsatt for bruken. I tillegg bør bruk av systemer for biometrisk fjernidentifikasjon i sanntid på offentlig tilgjengelige steder med henblikk på rettshåndhevelse iverksettes bare for å bekrefte identiteten til den personen som bruken er spesifikt rettet mot, og bør begrenses til det som er strengt nødvendig når det gjelder tidsperioden samt det geografiske anvendelsesområdet og de personene som omfattes, særlig i betraktning av bevisene eller indikasjonene vedrørende truslene, ofrene eller gjerningspersonen. Bruk av systemet for biometrisk fjernidentifikasjon i sanntid på offentlig tilgjengelige steder bør tillates bare dersom den relevante rettshåndhevende myndigheten har foretatt en konsekvensanalyse om grunnleggende rettigheter, og med mindre annet er fastsatt i denne forordningen, har registrert systemet i EU-databasen som fastsatt i denne forordningen. Referansedatabasen over personer bør være formålstjenlig for hvert enkelt brukstilfelle i hver av situasjonene nevnt ovenfor.
- 35) Enhver bruk av et system for biometrisk fjernidentifikasjon i sanntid på offentlig tilgjengelige steder med henblikk på rettshåndhevelse bør være gjenstand for en uttrykkelig og særskilt tillatelse fra en rettsmyndighet eller en uavhengig forvaltningsmyndighet i en medlemsstat, hvis beslutning er bindende. Denne tillatelsen bør i prinsippet innhentes før KI-systemet brukes for å identifisere en eller flere personer. Det bør gis unntak fra denne regelen i behørig begrunnede hastetilfeller, det vil si i situasjoner der behovet for å bruke de aktuelle systemene er av en slik art at det er praktisk og objektivt umulig å innhente tillatelse før bruken av KI-systemet påbegynnes. I slike hastetilfeller bør bruken av KI-systemet begrenses til det absolutte minimumet som er nødvendig, og bør omfattes av hensiktsmessige garantier og vilkår som fastsatt i nasjonal rett og spesifisert av den rettshåndhevende myndigheten selv i forbindelse med hvert enkelt hastetilfelle. Dessuten bør den rettshåndhevende myndigheten i slike situasjoner anmode om en slik tillatelse med angivelse av grunnene til at den ikke har kunne anmode om den tidligere, uten ugrunnet opphold og senest innen 24 timer. Dersom slik tillatelse nektes, bør den bruken av systemer for biometrisk fjernidentifikasjon i sanntid som er knyttet til tillatelsen, umiddelbart bringes til opphør, og alle data som er knyttet til denne bruken, bør kasseres og slettes. Slike data omfatter inndata som er innhentet direkte av et KI-system under bruken av det, og resultatene og utdataene fra bruken knyttet til nevnte tillatelse. Den bør ikke omfatte inndata som er lovlig innhentet i samsvar med annen unionsrett eller nasjonal rett. I alle tilfeller bør ingen beslutning som har en negativ rettsvirkning for en person, treffes utelukkende på grunnlag av utdataene fra systemet for biometrisk fjernidentifikasjon.

⁽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).

- 36) For å kunne utføre sine oppgaver i samsvar med de kravene som er fastsatt i denne forordningen og i nasjonale regler, bør den relevante markedstilsynsmyndigheten og den nasjonale personvernmyndigheten underrettes om enhver bruk av systemet for biometrisk identifikasjon i sanntid. Markedstilsynsmyndighetene og de nasjonale personvernmyndighetene som er blitt underrettet, bør framlegge en årlig rapport for Kommisjonen om bruken av systemer for biometrisk identifikasjon i sanntid.
- 37) Dessuten bør det fastsettes, innenfor de uttømmende rammene fastsatt ved denne forordningen, at slik bruk på en medlemsstats territorium i samsvar med denne forordningen bør være mulig bare dersom og i den grad den berørte medlemsstaten har besluttet å uttrykkelig gi mulighet for å tillate slik bruk i sine nærmere regler i nasjonal rett. Dermed står medlemsstatene etter denne forordningen fritt til ikke å fastsette noen slik mulighet eller til bare å fastsette en slik mulighet for noen av de målene som i samsvar med denne forordningen kan begrunne at bruken tillates. Kommisjonen bør underrettes om slike nasjonale regler innen 30 dager etter at de er vedtatt.
- 38) Bruk av KI-systemer til biometrisk fjernidentifikasjon i sanntid av fysiske personer på offentlig tilgjengelige steder med henblikk på rettshåndhevelse innebærer nødvendigvis behandling av biometriske opplysninger. De reglene i denne forordningen 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 vil dermed regulere slik bruk og den tilhørende behandlingen av biometriske opplysninger på en uttømmende måte. Derfor bør slik bruk og behandling være mulig bare i den utstrekningen den er forenlig med rammen som fastsettes ved denne forordningen, uten at vedkommende myndigheter har rom utenfor denne rammen, dersom de opptrer for rettshåndhevelsesformål, til å bruke slike systemer og behandle slike data i den forbindelse, av de grunnene som er angitt i artikkel 10 i direktiv (EU) 2016/680. I denne sammenhengen er ikke denne forordningen ment å utgjøre det rettslige grunnlaget for behandling av personopplysninger i henhold til artikkel 8 i direktiv (EU) 2016/680. Bruk av systemer for biometrisk fjernidentifikasjon i sanntid på offentlig tilgjengelige steder for andre formål enn rettshåndhevelse, herunder av vedkommende myndigheter, bør imidlertid ikke omfattes av den særlige rammen for slik bruk med henblikk på rettshåndhevelse som er fastsatt i denne forordningen. Slik bruk for andre formål enn rettshåndhevelse bør derfor ikke være underlagt kravet om tillatelse etter denne forordningen og de gjeldende nærmere reglene i nasjonal rett som kan gi tillatelsen virkning.
- 39) Enhver behandling av biometriske opplysninger og andre personopplysninger i forbindelse med bruk av KI-systemer for biometrisk identifikasjon, unntatt i forbindelse med bruk av systemer for biometrisk fjernidentifikasjon i sanntid på offentlig tilgjengelige steder med henblikk på rettshåndhevelse, som er regulert ved denne forordningen, bør fortsatt oppfylle alle krav som følger av artikkel 10 i direktiv (EU) 2016/680. For andre formål enn rettshåndhevelse er behandling av biometriske opplysninger forbudt i henhold til artikkel 9 nr. 1 i forordning (EU) 2016/679 og artikkel 10 nr. 1 i forordning (EU) 2018/1725, med noen begrensede unntak som er fastsatt i nevnte artikler. Ved anvendelsen av artikkel 9 nr. 1 i forordning (EU) 2016/679 har nasjonale personvernmyndigheter allerede truffet beslutninger om å forby bruk av biometrisk fjernidentifikasjon for andre formål enn rettshåndhevelse.
- 40) I samsvar med artikkel 6a i protokoll nr. 21 om Det forente kongerikes og Irlands stilling med hensyn til området for frihet, sikkerhet og rettferdighet, som er tatt inn som vedlegg til TEU og TEUV, er Irland ikke bundet av reglene fastsatt i denne forordningens artikkel 5 nr. 1 første ledd bokstav g) i den utstrekning den får anvendelse på bruk 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 bruk av KI-systemer som omfattes av den bestemmelsen, artikkel 5 nr. 1 første ledd bokstav h), artikkel 5 nr. 2–6 og artikkel 26 nr. 10, som er vedtatt på grunnlag av artikkel 16 i TEUV om medlemsstatenes behandling av personopplysninger, når de utøver virksomhet som omfattes av tredje del av deling V kapittel 4 eller 5 i TEUV, når Irland ikke er bundet av regler om former for strafferettslig samarbeid eller politisamarbeid som krever overholdelse av de bestemmelsene som er 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 tatt inn som vedlegg til TEU og TEUV, er Danmark ikke bundet av reglene fastsatt i denne forordningens artikkel 5 nr. 1 første ledd bokstav g) i den utstrekning den får anvendelse på bruk 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 bruk av KI-systemer som omfattes av den bestemmelsen, artikkel 5 nr. 1 første ledd bokstav h), nr. 2–6) og artikkel 26 nr. 10), som er vedtatt

på grunnlag av artikkel 16 i TEUV, eller med forbehold om at de får anvendelse, om medlemsstatenes behandling av personopplysninger når de utøver virksomhet som omfattes av tredje del avdeling V kapittel 4 eller 5 i TEUV.

- 42) I tråd med uskyldspresumsjonen bør fysiske personer i Unionen alltid dømmes på grunnlag av sin faktiske atferd. Fysiske personer bør aldri dømmes ut fra KI-predikert atferd som er basert utelukkende på profilering av dem eller på deres personlighetstrekk eller kjennetegn, som for eksempel nasjonalitet, fødested, bosted, antall barn, gjeldsnivå eller type bil, uten en rimelig mistanke basert på objektive, verifiserbare fakta om at personen deltar i en kriminell virksomhet, og uten en menneskelig vurdering. Derfor bør det være forbud mot risikovurderinger av fysiske personer som foretas for å vurdere sannsynligheten for at de vil begå en overtredelse, eller for å forutsi en faktisk eller potensiell straffbar handling utelukkende på grunnlag av en profilering av personene eller en vurdering av deres personlighetstrekk og kjennetegn. I alle tilfeller omfatter eller berører ikke dette forbudet risikoanalyser som ikke er basert på profilering av enkeltpersoner eller på personlighetstrekkene og egenskapene til enkeltpersoner, for eksempel KI-systemer som bruker risikoanalyser til å vurdere sannsynligheten for økonomisk bedrageri fra foretak på grunnlag av mistenkelige transaksjoner, eller risikoanalyseverktøy til å forutsi sannsynligheten for at tollmyndighetene lokaliserer narkotika eller ulovlige varer, for eksempel på grunnlag av kjente smuglerruter.
- 43) Å bringe i omsetning, ta i bruk for dette bestemte formålet eller bruke KI-systemer som oppretter eller utvider ansikts-gjenkjenningsdatabaser gjennom ikke-måltrettet skraping av ansiktsbilder fra internett eller overvåkingskameraer, bør forbys, ettersom denne praksisen øker følelsen av masseovervåking og kan føre til grove brudd på grunnleggende rettigheter, herunder retten til personvern.
- 44) Det er stor uro rundt det vitenskapelige grunnlaget for KI-systemer som har som formål å identifisere eller utlede følelser, særlig fordi følelsesuttrykk varierer betydelig på tvers av kulturer og situasjoner, og endog hos en og samme person. Blant de viktigste svakhetene ved slike systemer er den begrensede påliteligheten, mangelen på spesifisitet og den begrensede generaliserbarheten. Derfor kan KI-systemer som identifiserer eller utleder fysiske personers følelser eller intensjoner på grunnlag av deres biometriske opplysninger, få diskriminerende utfall og gripe inn i de berørte personenes rettigheter og friheter. Tatt i betraktning maktubalansen innenfor arbeid og utdanning, kombinert med disse systemenes inngripende natur, kan slike systemer føre til skadelig eller ufordelaktig behandling av visse fysiske personer eller hele grupper av fysiske personer. Derfor bør det forbys å bringe i omsetning, ta i bruk eller bruke KI-systemer som er beregnet på å fange opp enkeltpersoners emosjonelle tilstand i situasjoner knyttet til arbeidsplassen eller utdanningsstedet. Dette forbudet bør ikke omfatte KI-systemer som bringes i omsetning utelukkende av medisinske eller sikkerhetsmessige årsaker, for eksempel systemer som er beregnet på terapeutisk bruk.
- 45) Praksis som er forbudt etter unionsretten, herunder regelverket for vern av personopplysninger, ikke-diskriminering og forbrukervern, bør ikke berøres av denne forordningen.
- 46) KI-systemer med høy risiko bør bare bringes i omsetning på unionsmarkedet, tas i bruk eller brukes dersom de oppfyller visse obligatoriske krav. Disse kravene bør sikre at KI-systemer med høy risiko som er tilgjengelige i Unionen, eller der utdataene på annen måte brukes i Unionen, ikke utgjør en uakseptabel risiko for viktige allmenne interesser i Unionen som er anerkjent og beskyttet av unionsretten. På grunnlag av den nye rettslige rammen, som avklart i kommisjonsmeldingen om den blå veiledningen («Blue Guide») om gjennomføring av EUs produktregler 2022⁽²⁰⁾, er hovedregelen at mer enn én rettsakt i EU-harmoniseringsregelverket, slik som europaparlaments- og rådsforordning (EU) 2017/745⁽²¹⁾ og (EU) 2017/746⁽²²⁾ eller europaparlaments- og rådsdirektiv 2006/42/EF⁽²³⁾, kan få anvendelse på ett og samme produkt, ettersom produktet bare kan gjøres tilgjengelig eller tas i bruk når det oppfyller alt gjeldende EU-harmoniseringsregelverk. For å sikre konsekvens og unngå unødvendige administrative byrder eller kostnader bør leverandører av et produkt som inneholder ett eller flere KI-systemer med høy risiko og omfattes av kravene i denne forordningen og av EU-harmoniseringsregelverket angitt i et vedlegg til denne forordningen, ha fleksibilitet når det gjelder å

⁽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 samt 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).

treffe driftsmessige beslutninger om hvordan det skal sikres at et produkt som inneholder ett eller flere KI-systemer, oppfyller alle gjeldende krav i EU-harmoniseringsregelverket på en optimal måte. KI-systemer som identifiseres som systemer med høy risiko, bør begrenses til systemer som har en betydelig skadevirkning på helsen, sikkerheten og de grunnleggende rettighetene til personer i Unionen, og denne begrensningen bør minimere enhver potensiell begrensning av internasjonal handel.

- 47) KI-systemer kan ha en negativ innvirkning på personers helse og sikkerhet, særlig når slike systemer fungerer som sikkerhetskomponenter i produkter. I samsvar med målene i EUs harmoniseringsregelverk om å lette fritt varebytte i det indre marked og sørge for at bare produkter som er sikre og for øvrig oppfyller kravene, finner veien ut på markedet, er det viktig at den sikkerhetsrisikoen som et produkt i sin helhet kan skape på grunn av sine digitale komponenter, herunder KI-systemer, forebygges og reduseres på behørig måte. For eksempel bør stadig mer autonome roboter, enten i sammenheng med produksjon eller personlig assistanse og pleie, kunne operere trygt og utføre sine funksjoner i komplekse miljøer. Også i helsesektoren, der liv og helse i særlig grad står på spill, bør de stadig mer avanserte diagnosesystemene og systemene til støtte for menneskelige beslutninger være pålitelige og nøyaktige.
- 48) Omfanget av KI-systemets negative innvirkning på de grunnleggende rettighetene som er beskyttet av pakten, er spesielt relevant ved klassifisering av et KI-system som et system med høy risiko. Disse rettighetene omfatter retten til menneskerverd, respekt for privatliv og familieliv, beskyttelse av personopplysninger, ytrings- og informasjonsfrihet, forsamlings- og foreningsfrihet, retten til ikke-diskriminering, retten til utdanning, forbrukervern, arbeidstakerrettigheter, rettighetene til personer med funksjonsnedsettelse, likestilling mellom kjønnene, immaterielle rettigheter, retten til effektive rettsmidler og til en rettferdig rettergang, retten til et forsvar, uskyldspresumpsjonen og retten til god forvaltning. I tillegg til disse rettighetene er det viktig å framheve at barn har særlige rettigheter som er nedfelt i artikkel 24 i pakten og i De forente nasjoners konvensjon om barnets rettigheter (UNCRC), videreutviklet i generell kommentar nr. 25 om det digitale miljøet, som begge krever at det tas hensyn til barns sårbarhet, og at de gis den beskyttelsen og omsorgen som er nødvendig for deres velferd. Den grunnleggende retten til et høyt nivå for miljøvern som er nedfelt i pakten og gjennomføres i Unionens politikk, bør også tas i betraktning ved vurdering av alvorlighetsgraden av den skaden et KI-system kan forårsake, herunder på menneskers helse og sikkerhet.
- 49) Når det gjelder KI-systemer med høy risiko som er sikkerhetskomponenter i produkter eller systemer, eller som i seg selv er produkter eller systemer som faller inn under virkeområdet for europaparlaments- og rådsforordning (EF) nr. 300/2008⁽²⁴⁾, europaparlaments- og rådsforordning (EU) nr. 167/2013⁽²⁵⁾, europaparlaments- og rådsforordning (EU) nr. 168/2013⁽²⁶⁾, europaparlaments- og rådsdirektiv 2014/90/EU⁽²⁷⁾, europaparlaments- og rådsdirektiv (EU) 2016/797⁽²⁸⁾, europaparlaments- og rådsforordning (EU) 2018/858⁽²⁹⁾, europaparlaments- og rådsforordning (EU) 2018/1139⁽³⁰⁾ og europaparlaments- og rådsforordning (EU) 2019/2144⁽³¹⁾, bør disse rettsaktene endres for å sikre at

⁽²⁴⁾ Europaparlaments- og rådsforordning (EF) nr. 300/2008 av 11. mars 2008 om felles bestemmelser om sikkerhet i 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 av og markedstilsyn for jordbruks- 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 av og markedstilsyn for to- eller trehjuls kjøretøyer og firehjuls motorsykler (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 samtrafikkveien i Den europeiske unions jernbanesystem (EUT L 138 av 26.5.2016, s. 44).

⁽²⁹⁾ Europaparlaments- og rådsforordning (EU) 2018/858 av 30. mai 2018 om godkjenning av og markedstilsyn med motorvogner og deres tilhengere samt systemer, komponenter og separate tekniske enheter til 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).

⁽³⁰⁾ Europaparlaments- og rådsforordning (EU) 2018/1139 av 4. juli 2018 om felles regler for sivil luftfart og om opprettelse av Den europeiske unions flysikkerhetsbyrå, og om endring av europaparlaments- og rådsforordning (EF) nr. 2111/2005, (EF) nr. 1008/2008, (EU) nr. 996/2010 og (EU) nr. 376/2014, og europaparlaments- og rådsdirektiv 2014/30/EU og 2014/53/EU, samt 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).

⁽³¹⁾ Europaparlaments- og rådsforordning (EU) 2019/2144 av 27. november 2019 om krav til typegodkjenning av motorvogner og deres tilhengere, og av systemer, komponenter og separate tekniske enheter beregnet på slike kjøretøyer, med hensyn til deres generelle sikkerhet og beskyttelse av personer i motorvognen og sårbare trafikanter, om endring av europaparlaments- og rådsforordning (EU) 2018/858 og om oppheving av europaparlaments- og rådsforordning (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. 1009/2010, (EU) nr. 19/2011, (EU) nr. 109/2011, (EU) nr. 458/2011, (EU) nr. 65/2012, (EU) nr. 130/2012, (EU) nr. 347/2012, (EU) nr. 351/2012, (EU) nr. 1230/2012 og (EU) 2015/166 (EUT L 325 av 16.12.2019, s. 1).

Kommisjonen på bakgrunn av de tekniske og reguleringsmessige særtrekkene ved hver sektor og uten å gripe inn i eksisterende mekanismer og myndigheter på området forvaltning, samsvarsvurdering og håndhevelse som er opprettet ved disse rettsaktene, tar hensyn til de obligatoriske kravene til KI-systemer med høy risiko som fastsettes i denne forordningen, når den vedtar relevante delegerte rettsakter eller gjennomføringsrettsakter på grunnlag av disse rettsaktene.

- 50) Når det gjelder KI-systemer som er sikkerhetskomponenter i produkter, eller i seg selv er produkter, som faller innenfor virkeområdet for bestemte deler av EU-harmoniseringsregelverket som er angitt i et vedlegg til denne forordningen, bør de klassifiseres som KI-systemer med høy risiko henhold til denne forordningen dersom det aktuelle produktet gjennomgår samsvarsvurderingsprosedyren med et tredjeparts samsvarsvurderingsorgan i henhold til nevnte relevante EU-harmoniseringsregelverk. Det dreier seg særlig om slike produkter som maskiner, leketøy, heiser, utstyr og sikringssystemer til bruk i eksplosjonsfarlige omgivelser, radioutstyr, trykkutstyr, fritidsbåtutstyr, taubaneanlegg, gassapparater, medisinsk utstyr, medisinsk utstyr til *in vitro*-diagnostikk, bilprodukter og luftfartsprodukter.
- 51) At et KI-system klassifiseres som et KI-system med høy risiko i henhold til denne forordningen, bør ikke nødvendigvis bety at produktet der KI-systemet er sikkerhetskomponent, eller KI-systemet i seg selv som produkt, anses for å ha høy risiko etter kriteriene fastsatt i det relevante EU-harmoniseringsregelverket som gjelder for produktet. Dette gjelder særlig for forordning (EU) 2017/745 og (EU) 2017/746, der det er fastsatt samsvarsvurdering utført av tredjepart for produkter med middels og høy risiko.
- 52) Når det gjelder frittstående KI-systemer, det vil si andre KI-systemer med høy risiko enn dem som er sikkerhetskomponenter i produkter eller selv er produkter, bør de klassifiseres som KI-systemer med høy risiko dersom de på grunn av sitt tiltenkte formål utgjør en høy risiko for skade på menneskers helse og sikkerhet eller grunnleggende rettigheter, tatt i betraktning både alvorlighetsgraden av den mulige skaden og sannsynligheten for at den oppstår, og dersom de brukes på en rekke spesifikt forhåndsdefinerte områder angitt i denne forordningen. Identifikasjonen av disse systemene er basert på de samme metodene og kriteriene som forutsettes også for eventuelle framtidige endringer i listen over KI-systemer med høy risiko, som Kommisjonen bør gis myndighet til å vedta gjennom delegerte rettsakter, for å ta hensyn til det raske tempoet i den teknologiske utviklingen samt potensielle endringer i bruken av KI-systemer.
- 53) Det er også viktig å presisere at det kan finnes særlige tilfeller der KI-systemer som det vises til i forbindelse med forhåndsdefinerte områder angitt i denne forordningen, ikke medfører en betydelig risiko for skade på de rettslige interessene som er vernet på disse områdene, fordi de ikke i vesentlig grad påvirker beslutningsprosessen eller ikke i vesentlig grad skader disse interessene. I denne forordningen bør et KI-system som ikke har vesentlig innvirkning på utfallet av beslutningstaking, forstås som et KI-system som ikke har innvirkning på innholdet i og dermed utfallet av beslutningstakingen, uansett om den er menneskelig eller automatisert. Et KI-system som ikke i vesentlig grad påvirker utfallet av beslutningstakingen, kan omfatte situasjoner der ett eller flere av de følgende vilkårene er oppfylt. Det første vilkåret bør være at KI-systemet er beregnet på å utføre en snever prosedyremessig oppgave, slik som 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 påvise dubletter i et stort antall søknader. Disse oppgavene er av så snever og begrenset art at de bare utgjør en begrenset risiko som ikke øker ved bruk av et KI-system i en sammenheng som er oppført som bruk med høy risiko i et vedlegg til denne forordningen. Det andre vilkåret bør være at oppgaven som utføres av KI-systemet, er beregnet på å forbedre resultatet av en tidligere fullført menneskelig aktivitet som kan være relevant for de formene for høyrisikobruk som er angitt i et vedlegg til denne forordningen. Tatt i betraktning disse egenskapene tilfører KI-systemet bare et ekstra lag til en menneskelig aktivitet, og dermed reduseres risikoen. Dette vilkåret vil for eksempel gjelde for KI-systemer som er beregnet på å forbedre språket i tidligere utarbeidede dokumenter, for eksempel med hensyn til profesjonell tone, akademisk språkbruk eller ved å tilpasse tekst til et bestemt merkevarebudskap. Det tredje vilkåret bør være at KI-systemet er beregnet på å påvise beslutningsmønstre eller avvik fra tidligere beslutningsmønstre. Risikoen vil bli redusert fordi bruken av KI-systemet følger en tidligere fullført menneskelig vurdering som det ikke er ment å erstatte eller påvirke uten tilbørlig menneskelig gjennomgang. Slike KI-systemer kan for eksempel være syste-

mer som ut fra et bestemt karaktersettingsmønster hos en lærer kan brukes til å kontrollere i ettertid om læreren kan ha avviket fra mønsteret, for å påvise eventuelle uoverensstemmelser eller uregelmessigheter. Det fjerde vilkåret bør være at KI-systemet er beregnet på å utføre en forberedende oppgave til en vurdering som er relevant for de KI-systemene som er angitt i et vedlegg til denne forordningen, noe som gjør den mulige virkningen av systemets utdata svært lav når det gjelder å utgjøre en risiko for den etterfølgende vurderingen. Dette vilkåret omfatter blant annet smarte løsninger for filhåndtering, som omfatter ulike funksjoner som indeksering, søk, tekst- og talebehandling eller kobling av data til andre datakilder, eller KI-systemer som brukes til oversettelse av kildedokumenter. I alle tilfeller bør KI-systemer som brukes i brukstilfeller med høy risiko som er oppført i et vedlegg til denne forordningen, anses å utgjøre en betydelig risiko for skade på helse, sikkerhet eller grunnleggende rettigheter dersom KI-systemet innbefatter profilering som definert i artikkel 4 nr. 4 i forordning (EU) 2016/679, artikkel 3 nr. 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 er et KI-system med høy risiko på grunnlag av vilkårene nevnt ovenfor, utarbeide dokumentasjon for denne vurderingen før systemet bringes i omsetning eller tas i bruk, og framlegge denne dokumentasjonen for de nasjonale vedkommende myndighetene på anmodning. En slik leverandør bør være forpliktet til å registrere KI-systemet i EU-databasen som opprettes i henhold til denne forordningen. Med sikte på å gi ytterligere veiledning om den praktiske gjennomføringen av vilkårene for at KI-systemene som er oppført i et vedlegg til denne forordningen, unntaksvis ikke er systemer med høy risiko, bør Kommisjonen etter samråd med KI-rådet fastsette retningslinjer for denne praktiske gjennomføringen, supplert med en omfattende liste over praktiske eksempler på brukstilfeller av KI-systemer som har høy risiko, og brukstilfeller som ikke har det.

- 54) Ettersom biometriske opplysninger utgjør en særlig kategori av personopplysninger, bør flere kritiske brukstilfeller av biometriske systemer klassifiseres som brukstilfeller med høy risiko, i den grad det er tillatt å bruke dem i henhold til relevant unionsrett og nasjonal rett. Tekniske unøyaktigheter i KI-systemer som er beregnet på biometrisk fjernidentifikasjon av fysiske personer, kan gi skjeve resultater og diskriminerende virkninger. Risikoen for slike mulige skjeve resultater og diskriminerende virkninger er særlig relevant når det gjelder alder, etnisitet, rase, kjønn eller funksjonsnedsettelse. Systemer for biometrisk fjernidentifikasjon bør derfor klassifiseres som systemer med høy risiko på grunn av risikoene forbundet med dem. En slik klassifisering utelukker KI-systemer som er ment å brukes til biometrisk verifisering, herunder autentisering, og hvis eneste formål er å bekrefte at en bestemt fysisk person er den som han eller hun utgir seg for å være, og å bekrefte identiteten til en fysisk person med det eneste formålet å få tilgang til en tjeneste, låse opp en enhet eller få sikker adgang til lokaler. I tillegg bør KI-systemer som er beregnet på å brukes til biometrisk kategorisering etter sensitive egenskaper eller kjennetegn som er beskyttet i samsvar med artikkel 9 nr. 1 i forordning (EU) 2016/679, på grunnlag av biometriske opplysninger, dersom disse ikke er forbudt i henhold til denne forordningen, og følelsesgjenkjenningssystemer som ikke er forbudt i henhold til denne forordningen, klassifiseres som systemer med høy risiko. Biometriske systemer som er beregnet på bruk utelukkende med det formålet å muliggjøre tiltak for cybersikkerhet og vern av personopplysninger, bør ikke anses som KI-systemer med høy risiko.

- 55) Når det gjelder forvaltning og drift av kritisk infrastruktur, er det hensiktsmessig å klassifisere KI-systemer som er beregnet på å brukes som sikkerhetskomponenter i forvaltning og drift av kritisk digital infrastruktur som oppført i nr. 8 i vedlegget til direktiv (EU) 2022/2557, i veitrafikk og i forsyning av vann, gass, varme og elektrisitet, som systemer med høy risiko, ettersom svikt eller funksjonsfeil i disse kan sette personers liv og helse i fare i stor målestokk og føre til vesentlige forstyrrelser i den ordinære gjennomføringen av sosiale og økonomiske aktiviteter. Sikkerhetskomponenter i kritisk infrastruktur, herunder kritisk digital infrastruktur, er systemer som brukes til direkte å beskytte den fysiske integriteten til kritisk infrastruktur eller helse og sikkerhet for personer og eiendom, men som ikke er nødvendige for at systemet skal fungere. Svikt eller funksjonsfeil i slike komponenter kan direkte føre til risiko for den fysiske integriteten til

kritisk infrastruktur og dermed til risiko for personers helse og sikkerhet samt for eiendom. Komponenter som er beregnet på bruk utelukkende for cybersikkerhetsformål, bør ikke anses som sikkerhetskomponenter. Eksempler på sikkerhetskomponenter i slik kritisk infrastruktur kan være systemer for overvåking av vanntrykk eller systemer for styring av brannalarmer i skydatasentre.

- 56) Innføring av KI-systemer innenfor utdanning er viktig for å fremme digital utdanning og opplæring av høy kvalitet og for at alle lærende og lærere skal kunne tilegne seg og dele de nødvendige digitale ferdighetene og kvalifikasjonene, herunder mediekompetanse og kritisk tenkning, slik at de kan delta aktivt i økonomien, i samfunnet og i demokratiske prosesser. KI-systemer som brukes i utdanning eller yrkesopplæring, særlig for å bestemme adgang eller opptak, anviser personer til institusjoner eller programmer for utdanning og yrkesrettet opplæring på alle nivåer, evaluere personers læringsutbytte, vurdere hva som er et hensiktsmessig utdanningsnivå for en person, og vesentlig påvirke nivået på den utdanningen og opplæringen som enkeltpersoner vil motta eller gis tilgang til, eller overvåke og påvise forbudt atferd hos studenter under prøver, bør imidlertid klassifiseres som KI-systemer med høy risiko, ettersom de kan bestemme en persons utdannings- og yrkesforløp og derfor påvirke personens mulighet til å skaffe seg et levebrød. Når slike systemer utformes og brukes på en uhensiktsmessig måte, kan de være særlig inngripende og kan krenke retten til en utdanning og retten til ikke å bli diskriminert samt opprettholde historiske diskrimineringsmønstre, for eksempel mot kvinner, visse aldersgrupper, personer med funksjonsnedsettelse eller personer av en bestemt etnisk opprinnelse eller med en bestemt seksuell legning.
- 57) KI-systemer som brukes innenfor sysselsetting, arbeidsledelse og tilgang til selvstendig næringsvirksomhet, særlig til rekruttering og utvelgelse av personer og for å treffe beslutninger som påvirker vilkårene for det arbeidsrelaterte forholdet, for forfremmelser og oppsigelser i arbeidsrelaterte kontraktsforhold, til å fordele oppgaver på grunnlag av individuell atferd, personlighetstrekk eller egenskaper og til å overvåke eller evaluere personer i arbeidsrelaterte kontraktsforhold, bør også klassifiseres som systemer med høy risiko, ettersom disse systemene kan ha en betydelig innvirkning på framtidige karrieremuligheter, disse personenes livsgrunnlag og arbeidstakernes rettigheter. Relevante arbeidsrelaterte kontraktsforhold bør på en meningsfull måte involvere ansatte og personer som yter tjenester via plattformer som omhandlet i Kommisjonens arbeidsprogram for 2021. Gjennom hele rekrutteringsprosessen og når personer evalueres, forfremmes eller beholdes i arbeidsrelaterte kontraktsforhold, kan slike systemer opprettholde historiske diskrimineringsmønstre, for eksempel mot kvinner, visse aldersgrupper, personer med funksjonsnedsettelse eller personer av en bestemt etnisk opprinnelse eller med en bestemt seksuell legning. KI-systemer som brukes til å overvåke prestasjonene og atferden til slike personer, kan også undergrave deres grunnleggende rettigheter til vern av personopplysninger og til personvern.
- 58) Et annet område der bruk av KI-systemer fortjener særlig oppmerksomhet, er i forbindelse med tilgang til og utnyttelse av visse vesentlige private og offentlige tjenester og ytelser som er nødvendige for at folk skal kunne delta fullt ut i samfunnet eller forbedre sin levestandard. Særlig er fysiske personer som søker om eller mottar vesentlige offentlige bistandsytelser og -tjenester fra offentlige myndigheter, så som helsetjenester, trygdeytelser, sosiale tjenester som gir beskyttelse ved blant annet svangerskap og fødsel, sykdom, arbeidsulykker, omsorgsbehov, alderdom eller arbeidsløshet, samt sosialhjelp og boligstøtte, vanligvis avhengige av disse ytelsene og tjenestene og befinner seg i en sårbar stilling i forhold til de ansvarlige myndighetene. Dersom KI-systemer brukes til å avgjøre om slike ytelser og tjenester bør gis, nektes, reduseres, tilbakekalles eller kreves tilbake av myndighetene, herunder hvorvidt mottakerne har rettmessig krav på slike ytelser eller tjenester, kan disse systemene ha en betydelig innvirkning på personers livsgrunnlag og kan krenke deres grunnleggende rettigheter, slik som retten til sosialomsorg, ikke-diskriminering, menneskeverd eller effektive rettsmidler, og bør derfor klassifiseres som systemer med høy risiko. Likevel bør ikke denne forordningen hindre at det utvikles og brukes innovative metoder innenfor offentlig forvaltning, der man vil kunne dra nytte av en mer utstrakt bruk av sikre KI-systemer som er i samsvar med kravene, forutsatt at disse systemene ikke medfører høy risiko for juridiske og fysiske personer. Dessuten bør KI-systemer som brukes til å vurdere kredittskåren eller kredittverdigheten til fysiske personer, klassifiseres som KI-systemer med høy risiko, ettersom de avgjør disse personenes tilgang til økonomiske ressurser eller vesentlige tjenester som bolig, elektrisitet og telekommunikasjonstjenester. KI-systemer som brukes til disse formålene, kan føre til diskriminering av personer eller grupper og opprettholde historiske diskrimineringsmønstre, for eksempel på grunnlag av etnisk opprinnelse, kjønn, funksjonsnedsettelse, alder eller seksuell legning, eller skape nye former for diskriminering. KI-systemer som er fastsatt i unionsretten med henblikk på å avdekke bedrageri i forbindelse med tilbud av finansielle tjenester, og for tilsynsformål for å beregne kapitalkravene til kredittinstitusjoner og forsikringsforetak, bør imidlertid ikke anses som systemer med høy risiko etter denne forordningen. Dessuten kan KI-systemer som er beregnet på å brukes til risikovurdering og prissetting i forbindelse med helse- og

livsforsikring for fysiske personer, også ha en betydelig innvirkning på personers livsgrunnlag, og dersom de ikke utformes, utvikles og brukes på behørig måte, kan de krenke grunnleggende rettigheter og få alvorlige konsekvenser for menneskers liv og helse, herunder økonomisk utestenging og diskriminering. Endelig vil KI-systemer som brukes, herunder av politiet, brannvesenet og helsevesenet, til å evaluere og klassifisere nødansrop fra fysiske personer eller til å sende ut eller fastsette prioritet for utsending av beredskapstjenester, samt systemer for pasientsortering for førstehjelp, også klassifiseres som systemer med høy risiko, ettersom de treffer beslutninger i situasjoner som er svært kritiske for personers liv, helse og eiendom.

- 59) Med bakgrunn i de rettshåndhevende myndighetenes rolle og ansvar er deres tiltak, når de innebærer visse typer bruk av KI-systemer, kjennetegnet ved en betydelig grad av maktubalanse og kan føre til overvåking, pågripelse eller frihetsberøvelse av en fysisk person samt andre negative konsekvenser for grunnleggende rettigheter som garanteres i pakten. KI-systemet kan peke ut personer på en diskriminerende eller annen feilaktig eller urettferdig måte, særlig dersom det ikke er trent med data av høy kvalitet, ikke oppfyller passende krav til ytelse, nøyaktighet eller robusthet, eller ikke er riktig utformet og testet før det blir brakt i omsetning eller tatt i bruk på annen måte. Dessuten kan slike KI-systemer hindre utøvelsen av viktige grunnleggende rettigheter, slik som retten til effektive rettsmidler, retten til en rettferdig rettergang, retten til et forsvar og uskyldspresumpsjonen, særlig dersom systemene ikke er tilstrekkelig åpne, forklarbare og dokumentert. En rekke KI-systemer som er beregnet på å brukes i rettshåndhevelsessammenheng, der nøyaktighet, pålitelighet og åpenhet er særlig viktig for å unngå negative virkninger, opprettholde allmennhetens tillit og sikre ansvarlighet og effektive rettsmidler, bør derfor klassifiseres som systemer med høy risiko, i den grad det er tillatt å bruke dem i henhold til relevant unionsrett og nasjonal rett. På bakgrunn av aktivitetenes art og den risikoen som er forbundet med dem, bør disse KI-systemene med høy risiko særlig omfatte KI-systemer beregnet på å brukes av eller på vegne av rettshåndhevende myndigheter eller av Unionens institusjoner, organer, kontorer eller byråer som bistår de rettshåndhevende myndighetene, for å vurdere risikoen for at en fysisk person skal bli offer for straffbare handlinger, som løgndetektorer og lignende verktøy, for å vurdere påliteligheten av bevis i forbindelse med etterforskning eller rettsforfølgning av straffbare handlinger, og, dersom dette ikke er forbudt i henhold til denne forordningen, for å vurdere risikoen for at en fysisk person skal begå eller på nytt begå en straffbar handling, ikke bare på grunnlag av profilering av fysiske personer eller vurdering av personlighetstrekk og egenskaper eller fysiske personers eller grupper tidligere kriminelle atferd, til profilering i forbindelse med avsløring, etterforskning eller rettsforfølgning av straffbare handlinger. KI-systemer som er særskilt beregnet på å brukes i forvaltningssaker av skatte- og tollmyndighetene samt av enheter for finansiell etterretning som utfører forvaltningsoppgaver som omfatter analyse av opplysninger i samsvar med EUs anti-hvitvaskingsregelverk, bør ikke klassifiseres som KI-systemer med høy risiko som brukes av rettshåndhevende myndigheter med henblikk å forebygge, avsløre, etterforske og straffeforfølge straffbare forhold. Rettshåndhevende myndigheters og andre relevante myndigheters bruk av KI-verktøy bør ikke bli en faktor som bidrar til ulikhet eller utestenging. Den innvirkningen som bruk av KI-verktøy har på mistenktes rett til et forsvar, bør ikke overses, særlig ikke vanskelighetene med å skaffe meningsfull informasjon om disse systemenes virkemåte og dermed med å bestrebe resultatene fra verktøyene i retten, særlig for fysiske personer som er under etterforskning.
- 60) KI-systemer som brukes i migrasjons-, asyl- og grensekontrollforvaltning, berører personer som ofte er i en særlig sårbar stilling, og som er avhengige av utfallet av vedkommende offentlige myndigheters tiltak. Det er derfor særlig viktig at KI-systemer som brukes i disse sammenhengene, er nøyaktige, ikke-diskriminerende og åpne, for å sikre respekt for de berørte personenes grunnleggende rettigheter, særlig deres rett til fri bevegelighet, ikke-diskriminering, personvern og vern av personopplysninger, internasjonal beskyttelse og god forvaltning. KI-systemer bør derfor klassifiseres som systemer med høy risiko, i den grad det er tillatt å bruke dem i henhold til relevant unionsrett og nasjonal rett, når de er beregnet på å brukes av eller på vegne av vedkommende offentlige myndigheter eller av Unionens institusjoner, organer, kontorer eller byråer med ansvar for oppgaver på områdene migrasjons-, asyl- og grensekontrollforvaltning, slik som løgndetektorer og lignende verktøy, for å vurdere visse risikoer forbundet med fysiske personer som reiser inn på en medlemsstats territorium eller søker om visum eller asyl, for å bistå vedkommende offentlige myndigheter i behandlingen, herunder den tilhørende vurderingen av bevisenes pålitelighet, av søknader om asyl, visum og oppholdstillatelse og klager i den forbindelse, med det formålet å fastslå om fysiske personer som søker, er berettiget til slik status, med henblikk på å oppdage, gjenkjenne eller identifisere fysiske personer i forbindelse med migrasjons-, asyl- og grensekontrollforvaltning, med unntak av verifisering av reisedokumenter. KI-systemer på området migrasjons-, asyl- og grensekontrollforvaltning som omfattes av denne forordningen, bør oppfylle de relevante prosedyrekravene fastsatt i

europaparlaments- og rådsforordning (EF) nr. 810/2009⁽³²⁾, europaparlaments- og rådsdirektiv 2013/32/EU⁽³³⁾ og annen relevant unionsrett. KI-systemer bør ikke under noen omstendigheter brukes i migrasjons-, asyl- og grensekontrollforvaltning 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 stilling utferdiget i Genève 28. juli 1951, som endret ved protokollen av 31. januar 1967. De bør heller ikke brukes til på noen måte å krenke non-refoulement-prinsippet eller til å nekte sikre og effektive rettslige veier inn på Unionens territorium, herunder retten til internasjonal beskyttelse.

- 61) Visse KI-systemer som er beregnet på rettspleie og demokratiske prosesser, bør klassifiseres som systemer med høy risiko, ettersom de potensielt kan ha betydelig innvirkning på demokratiet, rettsstaten, individuelle friheter samt retten til effektive rettsmidler og en rettferdig rettergang. For å håndtere risikoen for potensielle skjevheter, feil og manglende åpenhet bør særlig KI-systemer som er beregnet på å brukes av eller på vegne av en rettsmyndighet for å bistå rettsmyndigheter med å undersøke og tolke fakta og regelverk og med å anvende regelverket på et konkret sett med fakta, klassifiseres som systemer med høy risiko. KI-systemer som er beregnet på å brukes av organer for alternativ tvisteløsning for disse formålene, bør også anses som systemer med høy risiko når resultatene av den alternative tvisteløsningsforhandlingen har rettsvirkninger for partene. Bruk av KI-verktøy kan støtte, men bør ikke erstatte dommernes beslutningsrett eller domstolenes uavhengighet; den endelige beslutningstakingen må fortsatt være en menneskedrevet aktivitet. Klassifiseringen av KI-systemer som systemer med høy risiko bør imidlertid ikke omfatte KI-systemer som er beregnet på rent underordnede administrative aktiviteter som ikke påvirker den faktiske rettspleien i enkeltsaker, slik som anonymisering eller pseudonymisering av rettsavgjørelser, dokumenter eller data, kommunikasjon mellom personell eller administrative oppgaver.
- 62) Uten at det berører reglene fastsatt i europaparlaments- og rådsforordning (EU) 2024/900⁽³⁴⁾, og for å håndtere risikoen for utilbørlig ekstern innblanding i stemmeretten som fastsatt i paktens artikkel 39 og negative virkninger på demokratiet og rettsstaten, bør KI-systemer som er beregnet på å brukes til å påvirke utfallet av et valg eller en folkeavstemning eller fysiske personers stemmeadfærd når de utøver sin stemmerett ved valg eller folkeavstemninger, klassifiseres som KI-systemer med høy risiko, med unntak av KI-systemer hvis utdata 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 KI-system med høy risiko i henhold til denne forordningen, bør ikke tolkes som en indikasjon på at bruk av systemet er lovlig i henhold til andre unionsrettsakter eller i henhold til nasjonal rett som er forenlig med unionsretten, for eksempel om vern av personopplysninger, bruk av løgnedetektorer og lignende verktøy eller andre systemer for å oppdage fysiske personers emosjonelle tilstand. Enhver slik bruk bør fortsatt skje utelukkende i samsvar med de gjeldende kravene som følger av paktens og av gjeldende avledet unionsrett og nasjonal rett. Denne forordningen bør ikke forstås slik at den fastsetter det rettslige grunnlaget for behandling av personopplysninger, herunder særlige kategorier av personopplysninger, dersom det er relevant, med mindre annet er uttrykkelig fastsatt i denne forordningen.
- 64) For å redusere risikoen ved KI-systemer med høy risiko som bringes i omsetning eller tas i bruk, og for å sikre et høyt troverdighetsnivå, bør det gjelde visse obligatoriske krav for KI-systemer med høy risiko, idet det tas hensyn til KI-systemets tiltenkte formål og sammenhengen det brukes i, og i samsvar med det risikostyringssystemet som leverandøren skal innføre. De tiltakene som leverandørene treffer for å oppfylle de obligatoriske kravene i denne forordningen, bør ta hensyn til det allment anerkjente aktuelle tekniske utviklingstrinnet for KI og bør være forholdsmessige og effektive når det gjelder å nå målene i denne forordningen. På grunnlag av den nye rettslige rammen, som avklart i kommi-

⁽³²⁾ Europaparlaments- og rådsforordning (EF) nr. 810/2009 av 13. juli 2009 om innføring av fellesskapsregler for visum (visumforordningen) (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 rundt og målretting av politisk reklame (EUT L, 2024/900, 20.3.2024, ELI: <http://data.europa.eu/eli/reg/2024/900/oj>).

sjonsmeldingen om den blå veiledningen («Blue Guide») om gjennomføring av EUs produktregler 2022, er hovedregelen at mer enn én rettsakt i EU-harmoniseringsregelverket kan få anvendelse på ett og samme produkt, ettersom produktet bare kan gjøres tilgjengelig eller tas i bruk når det oppfyller alt gjeldende EU-harmoniseringsregelverk. Farene ved KI-systemer som omfattes av kravene i denne forordningen, dreier seg om andre aspekter enn det eksisterende EU-harmoniseringsregelverket, og derfor vil kravene i denne forordningen utfylle det eksisterende EU-harmoniseringsregelverket. For eksempel kan maskiner eller medisinsk utstyr som inneholder et KI-system, være forbundet med risikoer som ikke omfattes av de grunnleggende helse- og sikkerhetskravene i det relevante harmoniserte unionsregelverket, ettersom denne sektorspesifikke retten ikke omhandler risikoer som er spesifikke for KI-systemer. Dette krever at de ulike rettsaktene anvendes samtidig og komplementært. For å sikre konsekvens og unngå unødvendige administrativ byrder og unødige kostnader bør leverandører av et produkt som inneholder ett eller flere KI-systemer med høy risiko, og som omfattes av kravene i denne forordningen samt av det EU-harmoniseringsregelverket basert på den nye rettslige rammen som er angitt i et vedlegg til denne forordningen, ha fleksibilitet når det gjelder å treffe driftsmessige beslutninger om hvordan det skal sikres at et produkt som inneholder ett eller flere KI-systemer, oppfyller alle gjeldende krav i nevnte EU-harmoniseringsregelverk på en optimal måte. Denne fleksibiliteten kan for eksempel innebære at leverandøren beslutter å integrere en del av de nødvendige test- og rapporteringsprosessene og den informasjonen og dokumentasjonen som kreves i henhold til denne forordningen, i allerede eksisterende dokumentasjon og prosedyrer som kreves i henhold til eksisterende EU-harmoniseringsregelverk som er basert på den nye rettslige rammen, og som er oppført i et vedlegg til denne forordningen. Dette bør ikke på noen måte undergrave leverandørens plikt til å overholde alle gjeldende krav.

- 65) Risikohåndteringssystemet bør bestå av en kontinuerlig, gjentakende prosess som planlegges og kjøres i hele livssyklusen til KI-systemet med høy risiko. Denne prosessen bør ta sikte på å identifisere og begrense de relevante risikoene ved KI-systemer når det gjelder helse, sikkerhet og grunnleggende rettigheter. Risikostyringssystemet bør gjennomgås og oppdateres regelmessig for å sikre at det fortsatt er effektivt, og at eventuelle vesentlige beslutninger og tiltak som treffes i henhold til denne forordningen, er begrunnet og dokumentert. Denne prosessen bør sikre at leverandøren identifiserer risikoer eller negative virkninger og iverksetter avbøtende tiltak for de kjente og rimelig forutsigbare risikoene ved KI-systemer når det gjelder helse, sikkerhet og grunnleggende rettigheter, i lys av deres tiltenkte formål og rimelig forutsigbar feilbruk, herunder mulige risikoer som oppstår som følge av samhandlingen mellom KI-systemet og miljøet det opererer i. Risikostyringssystemet bør omfatte de risikostyringstiltakene som er mest hensiktsmessige i lys av det aktuelle tekniske utviklingstrinnet for KI. Ved identifikasjon av de mest hensiktsmessige risikostyringstiltakene bør leverandøren dokumentere og forklare valgene som er gjort, og bør når det er relevant, involvere eksperter og eksterne berørte parter. Ved identifikasjon av rimelig forutsigbar feilbruk av KI-systemer med høy risiko bør leverandøren inkludere bruk av KI-systemer som, selv om den ikke direkte omfattes av det tiltenkte formålet som er angitt i bruksanvisningen, likevel er rimelig å forvente ut fra lett forutsigbar menneskelig atferd sett i sammenheng med de særskilte egenskapene ved og den særskilte bruken av et bestemt KI-system. Alle kjente eller forutsigbare omstendigheter som er knyttet til bruk av KI-systemet med høy risiko i samsvar med dets tiltenkte formål eller under forhold med rimelig forutsigbar feilbruk, og som kan føre til risiko for helse og sikkerhet eller grunnleggende rettigheter, bør inngå i bruksanvisningen fra leverandøren. Dette er for å sikre at idriftsetteren er klar over dem og tar hensyn til dem ved bruk av KI-systemet med høy risiko. Identifikasjon og iverksetting av risikoreduserende tiltak for forutsigbar feilbruk i samsvar med denne forordningen bør ikke innebære særskilt tilleggstrening av KI-systemet med høy risiko fra leverandørens side for å håndtere forutsigbar feilbruk. Leverandørene oppfordres imidlertid til å vurdere slike tilleggstreningstiltak for å redusere rimelig forutsigbar feilbruk, når det er nødvendig og hensiktsmessig.
- 66) KI-systemer med høy risiko bør omfattes av krav med hensyn til risikostyring, kvaliteten på og relevansen av datasett som brukes, teknisk dokumentasjon og registrering, åpenhet, informasjon til idriftsettere, 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 er tilgjengelige med rimelige midler, er ikke disse kravene uberettigede handelsbegrensninger.
- 67) Data av høy kvalitet og tilgang til slike spiller en avgjørende rolle i å skape struktur og i å sikre ytelsen til mange KI-systemer, særlig når det brukes teknikker som innebærer trening av modeller, med henblikk på å sikre at KI-systemet med høy risiko fungerer som tiltenkt og på en trygg måte, og at det ikke blir en kilde til diskriminering som er forbudt i

henhold til unionsretten. Datasett av høy kvalitet til trening, validering og testing krever at det innføres egnede rutiner for dataforvaltning og datahåndtering. Datasett til trening, validering og testing, herunder etikettene, bør være relevante, tilstrekkelig representative og så vidt mulig feilfrie og fullstendige med tanke på systemets tiltenkte formål. For å lette overholdelsen av unionsretten om vern av personopplysninger, så som forordning (EU) 2016/679, bør dataforvaltnings- og datahåndteringsrutinene når det gjelder personopplysninger, omfatte åpenhet om det opprinnelige formålet med datainnsamlingen. Datasettene bør også ha de hensiktsmessige statistiske egenskapene, herunder når det gjelder de personene eller gruppene av personer som KI-systemene med høy risiko er ment å brukes på, med særlig vekt på å redusere eventuelle skjevheter i datasettene som kan forventes å påvirke menneskers helse og sikkerhet, ha en negativ innvirkning på grunnleggende rettigheter eller føre til diskriminering som er forbudt etter unionsretten, særlig dersom utdata påvirker inndata til framtidige operasjoner (tilbakekoblingssløyfer). Skjevhetene kan for eksempel ligge innbakt i de underliggende datasettene, særlig når det brukes historiske data, eller de kan bli skapt når systemene implementeres under virkelige forhold. Resultater fra KI-systemer kan påvirkes av slike iboende skjevheter, som tenderer til å øke gradvis og dermed videreføre og forsterke eksisterende diskriminering, særlig mot personer som tilhører visse sårbare grupper, herunder rasemessige eller etniske grupper. Kravet om at datasettene skal være så fullstendige og feilfrie som mulig, bør ikke påvirke bruken av teknikker for å bevare personvernet i forbindelse med utvikling og testing av KI-systemer. Særlig bør datasett, i den grad deres tiltenkte formål krever det, ta hensyn til de egenskapene, kjennetegnene eller elementene som er særegne for de spesifikke geografiske, kontekstuelle, atferdsmessige eller funksjonelle omgivelsene der KI-systemet er ment å brukes. Kravene knyttet til dataforvaltning kan oppfylles ved å benytte tredjeparter som tilbyr sertifiserte etterlevelsestjenester, herunder verifisering av dataforvaltning, datasettintegritet samt praksis for trening, validering og testing av data, dersom det sikres at datakravene i denne forordningen oppfylles.

- 68) I forbindelse med utviklingen og vurderingen av KI-systemer med høy risiko bør visse aktører, som leverandører, meldte organer og andre relevante enheter, for eksempel europeiske digitale innovasjonsnav, test- og forsøksanlegg og forskere, kunne få tilgang til og bruke datasett av høy kvalitet innenfor sine respektive aktivitetsområder som er relatert til denne forordningen. Europeiske felles dataområder opprettet av Kommisjonen og tilrettelegging for datadeling mellom virksomheter og med myndigheter i allmennhetens interesse vil være avgjørende for å sikre pålitelig, ansvarlig og ikke-diskriminerende tilgang til data av høy kvalitet til trening, validering og testing av KI-systemer. Innenfor helse, for eksempel, vil det europeiske helsedataområdet muliggjøre ikke-diskriminerende tilgang til helsedata og trening av KI-algoritmer på disse datasettene på en måte som bevarer personvernet og er sikker, rettidig, åpen og pålitelig, og med hensiktsmessig institusjonell styring. Relevante vedkommende myndigheter, herunder sektormyndigheter, som gir eller støtter tilgangen til data, kan også bidra til at det leveres data av høy kvalitet til trening, validering og testing av KI-systemer.
- 69) Retten til personvern og vern av personopplysninger må sikres gjennom hele livssyklusen til KI-systemet. I den forbindelse gjelder prinsippene om dataminimering, innebygd personvern og personvern som standard, som fastsatt i unionsretten om vern av personopplysninger, når personopplysninger behandles. Tiltak som treffes av leverandører for å sikre samsvar med disse prinsippene, kan omfatte ikke bare anonymisering og kryptering, men også bruk av teknologi som gjør det mulig å innføre algoritmer i dataene og å trene KI-systemer uten å overføre selve rådataene eller de strukturerte dataene mellom partene eller å kopiere dem, uten at dette berører kravene til dataforvaltning fastsatt i denne forordningen.
- 70) For å ivareta andres rett til beskyttelse mot diskriminering som kan skyldes skjevheter i KI-systemer, bør leverandørene unntaksvis, i den utstrekning det er strengt nødvendig for å sikre påvisning og korrigering av skjevheter i forbindelse med KI-systemene med høy risiko, forutsatt at det gis tilstrekkelige garantier for fysiske personers grunnleggende rettigheter og friheter, og etter anvendelse av alle gjeldende vilkår fastsatt i denne forordningen samt vilkårene fastsatt i forordning (EU) 2016/679 og (EU) 2018/1725 og direktiv (EU) 2016/680, også kunne behandle særlige kategorier av personopplysninger, av hensyn til viktige allmenne interesser i henhold til artikkel 9 nr. 2 bokstav g) i forordning (EU) 2016/679 og artikkel 10 nr. 2 bokstav g) i forordning (EU) 2018/1725.
- 71) Å ha forståelig informasjon om hvordan KI-systemer med høy risiko er blitt utviklet og hvordan de yter gjennom hele sin levetid, er avgjørende for å gjøre disse systemene sporbare, for å verifisere at kravene i denne forordningen oppfylles, samt for overvåking av driften og overvåking etter omsetning. Dette krever at det føres registre, og at det finnes teknisk dokumentasjon tilgjengelig som inneholder den informasjonen som er nødvendig for å vurdere om KI-systemet oppfyller de relevante kravene, og for å lette overvåkingen etter omsetning. Denne informasjon bør omfatte systemets generelle egenskaper, kapasitet og begrensninger, algoritmer, data, trenings-, test- og valideringsprosesser som er brukt, samt dokumentasjon om det relevante risikostyringssystemet, og bør være avfattet i en klar og forståelig form. Den tekniske dokumentasjonen bør holdes tilstrekkelig oppdatert i hele KI-systemets levetid. Dessuten bør KI-systemer med høy risiko gjøre det teknisk mulig å registrere hendelser automatisk, ved hjelp av logger, i hele systemets levetid.

- 72) For å håndtere bekymringer knyttet til kompleksiteten og den manglende åpenheten i visse KI-systemer og hjelpe idriftsettere å oppfylle sine forpliktelser i henhold til denne forordningen bør det kreves at KI-systemer med høy risiko er åpne før de bringes i omsetning eller tas i bruk. KI-systemer med høy risiko bør utformes på en måte som gjør det mulig for idriftsettere å forstå hvordan KI-systemet fungerer, evaluere dets funksjonalitet og forstå hva som er dets styrker og begrensninger. KI-systemer med høy risiko bør ledsages av egnede opplysninger i form av en bruksanvisninger. Disse opplysningene bør omfatte KI-systemets egenskaper, funksjonalitet og ytelsesbegrensninger. Dette vil omfatte opplysninger om mulige kjente og forutsigbare omstendigheter ved bruken av KI-systemet med høy risiko, herunder handlinger fra idriftsetterens side som kan påvirke systemets virkemåte og ytelse, som innebærer at KI-systemet kan føre til risiko for helse, sikkerhet og grunnleggende rettigheter, om de endringene som er forhåndsbestemt og samsvarsvurdert av leverandøren, og om de relevante tiltakene for menneskelig tilsyn, herunder tiltakene for å lette idriftsetternes tolkning av utdataene fra KI-systemet. Åpenhet, også den medfølgende bruksanvisningen, bør hjelpe idriftsettere å bruke systemet og treffe informerte beslutninger. Idriftsettere bør blant annet bli bedre i stand til å velge det rette systemet til sin tiltenkte bruk ut fra de forpliktelsene som gjelder for dem, til å skaffe seg kunnskap om de tiltenkte og utelukkede bruksområdene for systemet og til å bruke KI-systemet riktig og når det er hensiktsmessig. For å gjøre informasjonen i bruksanvisningen mer lesbar og tilgjengelig bør det inkluderes illustrerende eksempler, for eksempel på begrensningene og på den tiltenkte og utelukkede bruken av KI-systemet. Leverandører bør sikre at all dokumentasjon, herunder bruksanvisningen, inneholder meningsfull, omfattende, tilgjengelig og forståelig informasjon, tatt i betraktning behovene og de forventede kunnskapene hos målgruppen av idriftsettere. Bruksanvisningen bør gjøres tilgjengelig på et språk som lett kan forstås av målgruppen av idriftsettere, som fastsatt av den aktuelle medlemsstaten.
- 73) KI-systemer med høy risiko bør utformes og utvikles på en slik måte at fysiske personer kan føre tilsyn med hvordan de fungerer, sikre at de brukes som tiltenkt, og at deres virkninger håndteres gjennom hele systemets livssyklus. For dette formålet bør leverandøren av systemet fastsette egnede tiltak for menneskelig tilsyn før systemet bringes i omsetning eller tas i bruk. Dersom det er relevant, bør slike tiltak særlig garantere at systemet er underlagt innebygde driftsrestriksjoner som ikke kan overstyres av systemet selv, og følger den menneskelige operatørens instruksjoner, samt at de fysiske personene som har fått i oppgave å føre menneskelig tilsyn, har den kompetansen, opplæringen og myndigheten som er nødvendig for å utføre denne oppgaven. Det er også avgjørende, alt etter hva som er relevant, å sikre at KI-systemer med høy risiko inneholder mekanismer for å veilede og informere en fysisk person som har fått i oppgave å føre menneskelig tilsyn, til å treffe informerte beslutninger om hvorvidt, når og hvordan de skal gripe inn for å unngå negative konsekvenser eller risikoer, eller å stoppe systemet dersom det ikke fungerer slik det var tenkt. Med tanke på de store konsekvensene det kan få for personer dersom visse biometriske identifikasjonssystemer identifiserer feilaktig, bør det fastsettes et strengere krav til menneskelig tilsyn for disse systemene, slik at idriftsetteren ikke kan treffe noen tiltak eller beslutninger på grunnlag av systemets identifikasjon med mindre denne er separat verifisert og bekreftet av minst to fysiske personer. Disse personene kan være fra en eller flere enheter og kan 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 forskjellige personene automatisk registreres i de loggene som genereres av systemet. Med tanke på de særlige forholdene på områdene rettshåndhevelse, migrasjon, grensekontroll og asyl bør dette kravet ikke gjelde når det etter unionsretten eller nasjonal rett anses uforholdsmessig å anvende det.
- 74) KI-systemer med høy risiko bør yte konsekvent gjennom hele sin livssyklus og oppfylle et passende nivå av nøyaktighet, robusthet og cybersikkerhet i lys av deres tiltenkte formål og i samsvar med det allment anerkjente aktuelle tekniske utviklingstrinnet. Kommisjonen og relevante organisasjoner og berørte parter oppfordres til å ta behørig hensyn til risikoreduksjon og KI-systemets negative virkninger. De forventede målene for ytelsesnivå bør angis i den medfølgende bruksanvisningen. Leverandørene oppfordres til å formidle denne informasjonen til idriftsetterne på en klar og lett forståelig måte, uten misforståelser eller villedende utsagn. Formålet med unionsretten om lovregulert måleteknikk, herunder europaparlaments- og rådsdirektiv 2014/31/EU⁽³⁵⁾ og 2014/32/EU⁽³⁶⁾, er å sikre at målingene er nøyaktige, og å bidra til åpenhet og rettferdighet i handelstransaksjoner. I denne sammenhengen bør Kommisjonen, alt etter hva som er relevant, og i samarbeid med relevante berørte parter og organisasjoner, for eksempel metrologi- og referansemålingsmyndigheter, oppmuntre til utvikling av referanseverdier og målemetoder for KI-systemer. I forbindelse med dette bør Kommisjonen lytte til og samarbeide med internasjonale partnere som arbeider med metrologi og relevante måleindikatorer knyttet til KI.

⁽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 måleinstrumenter (EUT L 96 av 29.3.2014, s. 149).

- 75) Teknisk robusthet er et sentralt krav til KI-systemer med høy risiko. De bør være motstandsdyktige mot skadelig eller på annen måte uønsket atferd som kan skyldes begrensninger i systemene eller i miljøet der systemene opererer (for eksempel feil, svikt, uoverensstemmelser eller uventede situasjoner). Derfor bør det treffes tekniske og organisatoriske tiltak for å sikre at KI-systemer med høy risiko er robuste, for eksempel ved å utforme og utvikle hensiktsmessige tekniske løsninger for å forebygge eller minimere skadelig eller på annen måte uønsket atferd. Disse tekniske løsningene kan for eksempel omfatte mekanismer som gjør at systemet kan avbryte sin drift på en sikker måte (feilsikre planer) ved visse uregelmessigheter eller når driften skjer utenfor visse forhåndsbestemte grenser. Manglende beskyttelse mot disse risikoene kan ha sikkerhetsmessige konsekvenser eller negativ innvirkning på de grunnleggende rettighetene, for eksempel på grunn av feilaktige beslutninger eller feil eller skjevheter i utdata som genereres av KI-systemet.
- 76) Cybersikkerhet spiller en avgjørende rolle for å sikre at KI-systemer er motstandsdyktige mot ondsinnede tredjeparters forsøk på å endre bruken av dem, deres virkemåte eller ytelse eller på å sette deres sikkerhetsegenskaper på spill ved å utnytte sårbarheter i systemene. Cyberangrep mot KI-systemer kan utnytte KI-spesifikke ressurser, slik som treningsdatasett (for eksempel ved dataforgiftning) eller trente modeller (for eksempel ved ondsinnede angrep eller utledning av tilhørighet («membership inference»)), eller utnytte sårbarheter i KI-systemets digitale ressurser eller den underliggende IKT-infrastrukturen. For å sikre et cybersikkerhetsnivå som står i forhold til risikoene, bør leverandører av KI-systemer med høy risiko derfor treffe egnede tiltak, for eksempel sikkerhetskontroller, idet de også tar hensyn til den underliggende IKT-infrastrukturen dersom det er relevant.
- 77) Uten at det berører de kravene til robusthet og nøyaktighet som er fastsatt i denne forordningen, kan KI-systemer med høy risiko som faller inn under virkeområdet for en europaparlaments- og rådsforordning om horisontale krav til cybersikkerhet for produkter med digitale elementer, etter nevnte forordning vise samsvar med kravene til cybersikkerhet i denne forordningen ved å oppfylle de grunnleggende kravene til cybersikkerhet i nevnte forordning. Når KI-systemer med høy risiko oppfyller de grunnleggende kravene i en europaparlaments- og rådsforordning om horisontale krav til cybersikkerhet for produkter med digitale elementer, bør de anses for å være i samsvar med kravene til cybersikkerhet i denne forordningen dersom oppfyllelsen av disse kravene er dokumentert i den EU-samsvarserklæringen eller de delene av den som er utstedt i henhold til nevnte forordning. For dette formålet bør det ved vurderingen av cybersikkerhetsrisikoen forbundet med et produkt med digitale elementer som er klassifisert som et KI-system med høy risiko i henhold til denne forordningen, som utføres i samsvar med en europaparlaments- og rådsforordning om horisontale krav til cybersikkerhet for produkter med digitale elementer, tas hensyn til risiko for et KI-systems cyberrobusthet når det gjelder uautoriserte tredjeparters forsøk på å endre bruken av systemet, dets virkemåte eller ytelse, herunder KI-spesifikke sårbarheter som dataforgiftning eller ondsinnede angrep samt, dersom det er relevant, risiko for grunnleggende rettigheter i samsvar med denne forordningen.
- 78) Samsvarsvurderingsprosedyren fastsatt i denne forordningen bør få anvendelse på de grunnleggende cybersikkerhetskravene til et produkt med digitale elementer som omfattes av en europaparlaments- og rådsforordning om horisontale cybersikkerhetskrav til produkter med digitale elementer, og som er klassifisert som et KI-system med høy risiko i henhold til denne forordningen. Denne regelen bør imidlertid ikke føre til en reduksjon i den nødvendige sikkerhetsgraden for kritiske produkter med digitale elementer som omfattes av en europaparlaments- og rådsforordning om horisontale cybersikkerhetskrav til produkter med digitale elementer. Som unntak fra denne regelen er derfor KI-systemer med høy risiko som faller inn under virkeområdet for denne forordningen, og som også er kvalifisert som viktige og kritiske produkter med digitale elementer i henhold til en europaparlaments- og rådsforordning om horisontale cybersikkerhetskrav til produkter med digitale elementer, og som samsvarsvurderingsprosedyren basert på internkontroll fastsatt i et vedlegg til denne forordningen får anvendelse på, underlagt bestemmelsene om samsvarsvurdering i en europaparlaments- og rådsforordning om horisontale cybersikkerhetskrav til produkter med digitale elementer når det gjelder de grunnleggende cybersikkerhetskravene i den forordningen. I så fall bør de respektive bestemmelsene om samsvarsvurdering basert på internkontroll som er fastsatt i et vedlegg til denne forordningen, få anvendelse på alle de andre aspektene som omfattes av denne forordningen. Med utgangspunkt i ENISAs kunnskap og ekspertise om cybersikkerhetspolitikk og de oppgavene som ENISA er tildelt i samsvar med europaparlaments- og rådsforordning (EU) 2019/881⁽³⁷⁾, bør Kommisjonen samarbeide med ENISA om spørsmål knyttet til cybersikkerhet i KI-systemer.

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

- 79) Det er hensiktsmessig at en spesifikk fysisk eller juridisk person, definert som leverandøren, påtar seg ansvaret for å bringe i omsetning eller ta i bruk et KI-system med høy risiko, uavhengig av om denne fysiske eller juridiske personen er den som har utformet eller utviklet systemet.
- 80) Som underskrivere av De forente nasjoners konvensjon om rettighetene til personer med nedsatt funksjonsevne er Unionen og medlemsstatene rettslig forpliktet til å beskytte personer med nedsatt funksjonsevne mot diskriminering og fremme deres likestilling, til å sikre at personer med nedsatt funksjonsevne på lik linje med andre har tilgang til informasjons- og kommunikasjonsteknologi og -systemer, og til å sikre personvernet til personer med nedsatt funksjonsevne. På bakgrunn av den økende betydningen og bruken av KI-systemer bør anvendelsen av prinsipper for universell utforming på alle nye teknologier og tjenester sikre full og lik tilgang for alle som potensielt er berørt av eller bruker KI-teknologi, herunder 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 europaparlaments- og rådsdirektiv (EU) 2016/2102⁽³⁸⁾ og direktiv (EU) 2019/882. Leverandørene bør sikre at disse kravene overholdes gjennom utforming. Derfor bør de nødvendige tiltakene i størst mulig grad være integrert i utformingen av KI-systemet.
- 81) Leverandøren bør etablere et forsvarlig kvalitetsstyringssystem, sikre at den nødvendige samsvarsvurderingsprosedyren er gjennomført, utarbeide den relevante dokumentasjonen og etablere et robust system for overvåking etter omsetning. Leverandører av KI-systemer med høy risiko som er underlagt forpliktelser med hensyn til kvalitetsstyringssystemer i henhold til relevant sektorspesifikk unionsrett, bør ha mulighet til å inkludere elementene i det kvalitetsstyringssystemet som fastsettes i denne forordningen, som en del av det eksisterende kvalitetsstyringssystemet fastsatt i nevnte sektorspesifikk unionsrett. Det bør også tas hensyn til komplementariteten mellom denne forordningen og eksisterende sektorspesifikk unionsrett i forbindelse med framtidig standardiseringsvirksomhet eller retningslinjer vedtatt av Kommisjonen. Offentlige myndigheter som tar i bruk KI-systemer med høy risiko til 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 relevant, idet det tas hensyn til sektorens særtrekk og den aktuelle offentlige myndighetens kompetanse og organisering.
- 82) For å gjøre det mulig å håndheve denne forordningen og skape like konkurransevilkår for operatørene, og tatt i betraktning 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 alle nødvendige opplysninger om et KI-systems samsvar med reglene. Før de gjør sine KI-systemer med høy risiko tilgjengelige i Unionen, bør derfor leverandører som er etablert i tredjeland, ved skriftlig fullmakt utpeke en bemyndiget representant som er etablert i Unionen. Denne bemyndigede representanten har en sentral rolle i å sikre at KI-systemer med høy risiko som bringes i omsetning eller tas i bruk i Unionen av leverandører som ikke er etablert i Unionen, oppfyller kravene, og i å fungere som leverandørenes kontaktperson i Unionen.
- 83) I lys av arten og kompleksiteten av verdikjeden for KI-systemer og i tråd med den nye rettslige rammen er det avgjørende å sikre rettslig forutsigbarhet og lette overholdelsen av denne forordningen. Det er derfor nødvendig å klargjøre rollen og de særlige forpliktelsene til relevante aktører i denne verdikjeden, for eksempel importører og distributører som kan bidra til utviklingen av KI-systemer. I visse situasjoner kan disse operatørene opptre i flere roller samtidig og bør derfor samlet sett oppfylle alle relevante forpliktelser knyttet til disse rollene. En operatør kan for eksempel opptre som distributør og importør samtidig.
- 84) For å sikre rettslig forutsigbarhet må det presiseres at under visse spesifikke vilkår bør enhver distributør, importør, idriftsetter eller annen tredjepart anses for å være en leverandør av et KI-system med høy risiko og derfor påta seg alle de relevante forpliktelsene. Dette vil være tilfellet dersom denne parten setter sitt navn eller varemerke på et KI-system med høy risiko som allerede er brakt i omsetning eller tatt i bruk, uten at det berører avtalefestede ordninger som fastsetter at forpliktelsene er fordelt annerledes. Det vil også være tilfellet dersom denne parten gjør en vesentlig endring av et KI-system med høy risiko som allerede er brakt i omsetning eller allerede er tatt i bruk, på en måte som gjør at det forblir et KI-system med høy risiko i samsvar med denne forordningen, eller dersom denne parten endrer det tiltenkte formålet med et KI-system, herunder et KI-system for allmenne formål, som ikke er klassifisert som et KI-system med høy risiko, og som allerede er brakt i omsetning eller tatt i bruk, på en måte som gjør at KI-systemet blir et KI-system med høy risiko i samsvar med denne forordningen. Disse bestemmelsene bør gjelde uten at det berører mer spesifikke bestemmelser fastsatt i visse deler av EU-harmoniseringsregelverket basert på den nye rettslige rammen, som denne forordningen bør anvendes sammen med. For eksempel bør artikkel 16 nr. 2 i forordning (EU) 2017/745, der det fastsettes

⁽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).

at visse endringer ikke skal anses for å utgjøre en endring av utstyr som kan påvirke utstyrets samsvar med gjeldende krav, fortsatt gjelde for KI-systemer med høy risiko som er medisinsk utstyr i henhold til definisjonen i den forordningen.

- 85) KI-systemer for allmenne formål kan brukes som KI-systemer med høy risiko alene eller som komponenter i andre KI-systemer med høy risiko. Derfor bør leverandørene av slike systemer, på grunn av systemenes særlige art og for å sikre en rettferdig ansvarsfordeling langs KI-verdikjeden, uansett om systemene som sådanne kan brukes som KI-systemer med høy risiko av andre leverandører eller som komponenter i KI-systemer med høy risiko, og med mindre annet er fastsatt i denne forordningen, samarbeide nært med leverandørene av de relevante KI-systemene med høy risiko, slik at de kan oppfylle de relevante forpliktelsene i henhold til denne forordningen, og med de vedkommende myndighetene som er etablert i henhold til denne forordningen.
- 86) Dersom den leverandøren som først brakte KI-systemet i omsetning eller tok det i bruk, ikke lenger bør anses som leverandør etter denne forordningen, og når denne leverandøren ikke uttrykkelig har utelukket at KI-systemet endres til et KI-system med høy risiko, bør førstnevnte leverandør likevel delta i et nært samarbeid og gjøre den nødvendige informasjonen tilgjengelig og gi den tekniske tilgangen som med rimelighet kan forventes, samt annen bistand som kreves for å oppfylle forpliktelsene i denne forordningen, særlig når det gjelder overholdelse av samsvarsvurderingen av KI-systemer med høy risiko.
- 87) Dersom et KI-system med høy risiko som er en sikkerhetskompont i et produkt som omfattes av EU-harmoniseringsregelverket basert på den nye rettslige rammen, ikke bringes i omsetning eller tas i bruk uavhengig av produktet, bør dessuten produkttilvirkeren definert i nevnte regelverk oppfylle leverandørens forpliktelser som fastsatt i denne forordningen og bør særlig sikre at KI-systemet som er innebygd i sluttproduktet, oppfyller kravene i denne forordningen.
- 88) Langs KI-verdikjeden er det ofte flere parter som leverer KI-systemer, -verktøy og -tjenester, men også komponenter eller prosesser som leverandøren har innarbeidet i KI-systemet for forskjellige formål, blant annet trening, omtrening, testing og evaluering av modeller, integrering i programvare eller andre aspekter av modellutvikling. Disse partene har en viktig rolle å spille i verdikjeden overfor leverandøren av det KI-systemet med høy risiko som deres KI-systemer, -verktøy, -tjenester, -komponenter eller -prosesser er integrert i, og bør etter skriftlig avtale gi denne leverandøren den informasjonen, kapasiteten, tekniske tilgangen og annen bistand som er nødvendig basert på det allment anerkjente aktuelle tekniske utviklingstrinnet, slik at leverandøren fullt ut kan oppfylle forpliktelsene fastsatt i denne forordningen uten å sette sine egne immaterielle rettigheter eller forretningshemmeligheter i fare.
- 89) Tredjeparter som gjør andre verktøy, tjenester, prosesser eller KI-komponenter enn KI-modeller for allmenne formål tilgjengelige for offentligheten, bør ikke være pålagt å oppfylle krav rettet mot ansvaret langs KI-verdikjeden, særlig overfor den leverandøren som har brukt eller integrert dem, når disse verktøyene, tjenestene, prosessene eller KI-komponentene gjøres tilgjengelige under fri lisens med åpen kildekode. Utviklere av andre verktøy, tjenester, prosesser eller KI-komponenter under fri lisens med åpen kildekode enn KI-modeller for allmenne formål bør oppfordres til å innføre allment akseptert dokumentasjonspraksis, for eksempel modellkort og datablader, som en måte å framskynde informasjonsdelingen langs KI-verdikjeden på, slik at det blir mulig å fremme pålitelige KI-systemer i Unionen.
- 90) Kommisjonen kan utvikle og anbefale frivillige standardvilkår for avtaler mellom leverandører av KI-systemer med høy risiko og tredjeparter som leverer verktøy, tjenester, komponenter eller prosesser som brukes eller integreres i KI-systemer med høy risiko, for å lette samarbeidet langs verdikjeden. Når Kommisjonen utvikler frivillige standardvilkår, bør den også ta hensyn til eventuelle avtalefestede krav som gjelder for bestemte sektorer eller virksomhetsscenarioer.
- 91) I betraktning av KI-systemenes karakter og den risikoen for sikkerheten og de grunnleggende rettighetene som kan være forbundet med bruken av dem, herunder med tanke på behovet for å sikre hensiktsmessig overvåking av ytelsen til et KI-system under virkelige forhold, bør det fastsettes særlige ansvarsområder for idriftsettere. Idriftsettere bør særlig treffe egnede tekniske og organisatoriske tiltak for å sikre at de bruker KI-systemer med høy risiko i samsvar med bruksanvisningen, og når det er relevant, bør det fastsettes visse andre forpliktelser med hensyn til overvåking av KI-systemenes virkemåte og med hensyn til registrering. Videre bør idriftsettere sikre at personene som er utpekt til å gjennomføre

bruksanvisningen og det menneskelige tilsynet som angitt i denne forordningen, har den nødvendige kompetansen, særlig tilstrekkelig KI-kompetanse, opplæring og myndighet til å utføre disse oppgavene på en forsvarlig måte. Disse forpliktelsene bør ikke berøre andre forpliktelser for idriftsettere i forbindelse med KI-systemer med høy risiko som følger av unionsretten eller nasjonal rett.

- 92) Denne forordningen berører ikke arbeidsgiveres plikt til å informere eller til å informere og konsultere arbeidstakere eller deres representanter i henhold til Unionens eller nasjonal rett og praksis, herunder europaparlaments- og rådsdirektiv 2002/14/EF ⁽³⁹⁾, om beslutninger om å ta i bruk eller bruke KI-systemer. Det må fortsatt sikres at arbeidstakerne og deres representanter blir informert om den planlagte idriftsettingen av KI-systemer med høy risiko på arbeidsplassen dersom vilkårene for denne informasjonsplikten eller informasjons- og konsultasjonsplikten i andre rettslige instrumenter ikke er oppfylt. Denne retten til å bli informert hører dessuten sammen med og er nødvendig for denne forordningens formål om å beskytte grunnleggende rettigheter. Derfor bør det fastsettes et informasjonskrav med henblikk på dette i denne forordningen, uten at det berører arbeidstakernes eksisterende rettigheter.
- 93) Risiko knyttet til KI-systemer kan skyldes måten de er utformet på, men også måten de brukes på. Distributører av KI-systemer med høy risiko spiller derfor en avgjørende rolle i å sikre at grunnleggende rettigheter beskyttes, og utfyller leverandørens forpliktelser i forbindelse med utviklingen av KI-systemet. Distributører har de beste forutsetningene for å forstå hvordan KI-systemet med høy risiko vil bli brukt i praksis, og kan derfor avdekke potensiell betydelig risiko som ikke har blitt forutsett i utviklingsfasen, takket være mer nøyaktig kunnskap om brukssammenhengen og hvilke personer eller grupper av personer som kan forventes å bli berørt, deriblant sårbare grupper. Idriftsettere av KI-systemer med høy risiko som er oppført i et vedlegg til denne forordningen, spiller også en avgjørende rolle i å informere fysiske personer, og når de treffer eller bistår i beslutninger som gjelder fysiske personer, bør de dersom det er relevant, informere de fysiske personene om at de er gjenstand for bruk av KI-systemet med høy risiko. Denne informasjonen bør omfatte det tiltenkte formålet og typen beslutninger som treffes. Idriftsetteren bør også informere de fysiske personene om deres rett til en forklaring som fastsatt i denne forordningen. Når det gjelder KI-systemer med høy risiko som brukes til rettshåndhevelsesformål, bør denne forpliktelsen gjennomføres i samsvar med artikkel 13 i direktiv (EU) 2016/680.
- 94) Enhver behandling av biometriske opplysninger som utføres i forbindelse med at KI-systemer brukes til biometrisk identifikasjon for rettshåndhevelsesformål, må være i samsvar med artikkel 10 i direktiv (EU) 2016/680, der det er fastsatt at slik behandling bare er tillatt dersom den er strengt nødvendig, forutsatt at det gis tilstrekkelige garantier for vern av den registrertes rettigheter og friheter, og dersom behandlingen er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett. Slik bruk må, når den er tillatt, også være i samsvar med prinsippene fastsatt i artikkel 4 nr. 1 i direktiv (EU) 2016/680, herunder lovlighet, rettferdighet og åpenhet, formålsbegrensning, nøyaktighet og lagringsbegrensning.
- 95) Uten at det berører gjeldende unionsrett, særlig forordning (EU) 2016/679 og direktiv (EU) 2016/680, bør bruk av systemer for biometrisk fjernidentifikasjon i ettertid være underlagt sikkerhetstiltak på grunn av disse systemenes inngripende natur. Systemer for biometrisk fjernidentifikasjon i ettertid bør alltid brukes på en måte som er forholdsmessig, legitim og strengt nødvendig, og dermed målrettet, når det gjelder hvilke mennesker som skal identifiseres samt stedet og tidsrommet, og være basert på et lukket datasett av lovlig ervervede videoopptak. Under alle omstendigheter bør systemer for biometrisk fjernidentifikasjon i ettertid ikke brukes i forbindelse med rettshåndhevelse på en måte som fører til til vilkårlig overvåking. Vilårene for biometrisk fjernidentifikasjon i ettertid bør ikke i noe tilfelle gi grunnlag for å omgå vilårene i forbudet mot og de strenge unntakene for biometrisk fjernidentifikasjon i sanntid.
- 96) For effektivt å sikre at grunnleggende rettigheter beskyttes, bør idriftsettere av KI-systemer med høy risiko som er offentligrettslige organer, eller private enheter som leverer offentlige tjenester, og idriftsettere av visse KI-systemer med høy risiko som er oppført i et vedlegg til denne forordningen, som bank- eller forsikringsenheter, gjennomføre en konsekvensanalyse om grunnleggende rettigheter før de tar systemene i bruk. Tjenester som er viktige for enkeltpersoner, og som er av offentlig karakter, kan også leveres av private enheter. Private enheter som leverer slike offentlige tjenester, er knyttet til oppgaver i allmennhetens interesse, for eksempel innen utdanning, helsetjenester, sosiale tjenester, boliger og rettspleie. Målet med konsekvensanalysen om grunnleggende rettigheter er at idriftsetteren skal avdekke de spesifikke risikoene for rettighetene til enkeltpersoner eller grupper av enkeltpersoner som kan forventes å bli berørt, og identifisere tiltak som skal treffes i tilfelle disse risikoene oppstår. Konsekvensanalysen bør utføres før KI-systemet med

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

høy risiko settes i drift, og bør oppdateres når idriftsetteren anser at noen av de relevante faktorene har endret seg. Konsekvensanalysen bør identifisere idriftsetterens relevante prosesser der KI-systemet med høy risiko vil bli brukt i tråd med sitt tiltenkte formål, og bør omfatte en angivelse av hvor lenge og med hvilken hyppighet systemet er ment å brukes, samt hvilke spesifikke kategorier av fysiske personer og grupper som kan forventes å bli berørt i den bestemte brukssammenheng. Analysen bør også avdekke særlige risikoer for skade som kan forventes å virke inn på de grunnleggende rettighetene til disse personene eller gruppene. Under gjennomføringen av denne analysen bør idriftsetteren ta hensyn til informasjon som er relevant for en tilfredsstillende vurdering av innvirkningen, herunder, men ikke begrenset til, den informasjonen som leverandøren av KI-systemet har gitt i bruksanvisningen. På grunnlag av de risikoene som avdekkes, bør idriftsetterne fastsette tiltak som skal treffes i tilfelle disse risikoene oppstår, herunder for eksempel styringsordninger i denne spesifikke brukssammenheng, eksempelvis ordninger for menneskelig tilsyn i samsvar med bruksanvisningen eller prosedyrer for klagebehandling og tvisteløsning, ettersom disse tiltakene kan bidra til å begrense risikoen for grunnleggende rettigheter i konkrete brukstilfeller. Etter å ha utført denne konsekvensanalysen bør idriftsetteren underrette den relevante markedstilsynsmyndigheten. Når det er hensiktsmessig, og for å innhente relevant informasjon som er nødvendig for å gjennomføre konsekvensanalysen, kan idriftsettere av KI-systemer med høy risiko, særlig når KI-systemer brukes i offentlig sektor, involvere relevante berørte parter, herunder representanter for grupper av personer som kan forventes å bli påvirket av KI-systemet, uavhengige eksperter og sivilsamfunnsorganisasjoner, i gjennomføringen av slike konsekvensanalyser og i utarbeidingen av tiltak som skal treffes i tilfelle risikoene oppstår. Det europeiske kontoret for kunstig intelligens (KI-kontoret) bør utvikle en mal for et spørreskjema med henblikk på å lette overholdelsen og redusere den administrative byrden for idriftsettere.

- 97) Begrepet KI-modeller for allmenne formål bør defineres klart og skilles fra begrepet KI-systemer, for å sikre rettslig forutsigbarhet. Definisjonen bør være basert på de viktigste funksjonelle egenskapene til en KI-modell for allmenne formål, særlig allmenngyldigheten og evnen til å utføre et bredt spekter av særskilte oppgaver på en kompetent måte. Disse modellene er vanligvis trent på store datamengder med forskjellige metoder, for eksempel selvovervåket, uovervåket eller forsterkende læring. KI-modeller for allmenne formål kan bringes i omsetning på ulike måter, blant annet via bibliotek, programmeringsgrensesnitt (API-er), som direkte nedlasting eller som fysiske kopier. Disse modellene kan ytterligere modifiseres eller finjusteres til nye modeller. Selv om KI-modeller er sentrale komponenter i KI-systemer, utgjør de ikke KI-systemer i seg selv. KI-modeller krever at det tilføyes ytterligere komponenter, som for eksempel et brukergrensesnitt, for å bli KI-systemer. KI-modeller er vanligvis integrert i og utgjør en del av KI-systemer. I denne forordningen fastsettes det særskilte regler for KI-modeller for allmenne formål og for KI-modeller for allmenne formål som innebærer systemrisiko, og disse reglene bør gjelde også når disse modellene er integrert i eller utgjør en del av et KI-system. Det bør forutsettes at forpliktelsene til leverandører av KI-modeller for allmenne formål får anvendelse så snart KI-modellene for allmenne formål bringes i omsetning. Når leverandøren av en KI-modell for allmenne formål integrerer en egen modell i sitt eget KI-system som gjøres tilgjengelig på markedet eller tas i bruk, bør denne modellen anses for å være brakt i omsetning, og derfor bør forpliktelsene for modeller i denne forordningen fortsatt gjelde i tillegg til forpliktelsene for KI-systemer. Forpliktelsene fastsatt for modeller bør i alle tilfeller ikke gjelde når en egen modell brukes til rent interne prosesser som ikke er avgjørende for å levere et produkt eller en tjeneste til tredjeparter, og når fysiske personers rettigheter ikke berøres. På grunn av sine potensielle vesentlig negative virkninger bør KI-modeller for allmenne formål med systemrisiko alltid være underlagt de relevante forpliktelsene i denne forordningen. Definisjonen bør ikke omfatte KI-modeller som brukes utelukkende til forsknings-, utviklings- og prototypingsaktiviteter før de bringes i omsetning. Dette berører ikke forpliktelsen til å overholde denne forordningen når en modell bringes i omsetning etter slike aktiviteter.
- 98) Samtidig som en modells allmenngyldighet også blant annet kan bestemmes ut fra en rekke parametere, bør modeller med minst en milliard parametere som er trent med en stor mengde data ved hjelp av selvovervåking i stor skala, anses for å vise betydelig allmenngyldighet og for å være i stand til på en kompetent måte å utføre et bredt spekter av særskilte oppgaver.
- 99) Store generative KI-modeller er et typisk eksempel på KI-modeller for allmenne formål, ettersom de muliggjør fleksibel generering av innhold, for eksempel i form av tekst, lyd, bilder eller video, som lett kan tilpasses et bredt spekter av særskilte oppgaver.
- 100) Når en KI-modell for allmenne formål er integrert i eller utgjør en del av et KI-system, bør dette systemet anses for å være et KI-system for allmenne formål når det, på grunn av denne integreringen, kan tjene en rekke ulike formål. Et KI-system for allmenne formål kan brukes direkte eller integreres i andre KI-systemer.

- 101) Leverandører av KI-modeller for allmenne formål spiller en særlig rolle og har et særlig ansvar langs KI-verdikjeden, ettersom modellene de leverer, kan danne grunnlag for en rekke nedstrømssystemer, ofte levert av nedstrømsleverandører, og dette krever god forståelse av modellene og deres kapasitet, både for at modellene skal kunne integreres i produktene deres, og for at de skal kunne oppfylle forpliktelsene sine i henhold til denne forordningen eller annet regelverk. Derfor bør det fastsettes forholdsmessige åpenhetstiltak, herunder at det skal utarbeides dokumentasjon som holdes oppdatert, og gis informasjon om KI-modellen for allmenne formål til nedstrømsleverandørene som skal bruke den. Teknisk dokumentasjon bør utarbeides og holdes oppdatert av leverandøren av KI-modellen for allmenne formål, slik at den på anmodning kan gjøres tilgjengelig for KI-kontoret og de nasjonale vedkommende myndighetene. De opplysningene som minst skal inngå i denne dokumentasjonen, bør fastsettes i særlige vedlegg til denne forordningen. Kommisjonen bør gis myndighet til å endre disse vedleggene ved hjelp av delegerte rettsakter på grunnlag av den teknologiske utviklingen.
- 102) Programvare og data, herunder modeller, som utgis under en fri lisens med åpen kildekode som tillater at de deles åpent, og der brukerne fritt kan få tilgang til, bruke, endre og om distribuere dem eller endrede versjoner av dem, kan bidra til forskning og nyskaping i markedet og gi betydelige vekstmuligheter for Unionens økonomi. KI-modeller for allmenne formål som er utgitt under fri lisens med åpen kildekode, bør anses for å sikre høy grad av åpenhet dersom deres parametere, herunder vektene, informasjonen om modellarkitekturen og informasjonen om modellbruken, gjøres offentlig tilgjengelige. Lisensen bør anses som fri med åpen kildekode også når den tillater brukere å kjøre, kopiere, distribuere, studere, endre og forbedre programvare og data, herunder modeller, under forutsetning av at den opprinnelige leverandøren av modellen krediteres, og at identiske eller sammenlignbare distribusjonsvilkår overholdes.
- 103) KI-komponenter under fri lisens med åpen kildekode omfatter programvare og data, herunder modeller og KI-modeller for allmenne formål, verktøy, tjenester eller prosesser i et KI-system. KI-komponenter med fri og åpen kildekode kan stilles til rådighet gjennom ulike kanaler, herunder ved at de utvikles i åpne programdatabaser. For denne forordningens formål bør KI-komponenter som leveres mot en pris eller på annen måte brukes til å generere inntekt, herunder gjennom levering av teknisk støtte eller andre tjenester, inkludert gjennom en programvareplattform, som er knyttet til KI-komponenten, og bruk av personopplysninger av andre grunner enn utelukkende for å forbedre programvarens sikkerhet, kompatibilitet eller interoperabilitet, med unntak av transaksjoner mellom svært små bedrifter, ikke omfattes av unntakene for KI-komponenter under fri lisens med åpen kildekode. At KI-komponenter gjøres tilgjengelige gjennom åpne programdatabaser, bør ikke i seg selv utgjøre generering av inntekt.
- 104) Leverandørene av KI-modeller for allmenne formål som utgis under fri lisens med åpen kildekode, og hvis parametere, herunder vektene, informasjonen om modellarkitekturen og informasjonen om modellbruken, gjøres offentlig tilgjengelige, bør være omfattet av unntak fra de kravene om åpenhet som gjelder for KI-modeller for allmenne formål, med mindre de kan anses å innebære systemrisiko, og i så fall bør ikke det forholdet at modellen er åpen og ledsaget av en lisens med åpen kildekode, anses for å være tilstrekkelig grunn til ikke å overholde forpliktelsene i henhold til denne forordningen. Ettersom det ved utgivelse av KI-modeller for allmenne formål under fri lisens med åpen kildekode ikke nødvendigvis avsløres vesentlig informasjon om datasettet som er brukt til trening eller finjustering av modellen, og om hvordan overholdelse av opphavsretten dermed er bitt sikret, bør unntaket for KI-modeller for allmenne formål fra å oppfylle kravene om åpenhet, under alle omstendigheter ikke gjelde plikten til å utarbeide et sammendrag av det innholdet som er brukt til modelltrening, og plikten til å innføre en framgangsmåte for å overholde Unionens regler om opphavsrett, særlig for å identifisere og etterleve forbeholdelse av rettigheter i henhold til artikkel 4 nr. 3 i europaparlaments- og rådsdirektiv (EU) 2019/790⁽⁴⁰⁾.
- 105) KI-modeller for allmenne formål, spesielt store generative KI-modeller, som er i stand til å generere tekst, bilder og annet innhold, skaper unike muligheter til nyskaping, men også utfordringer for kunstnere, forfattere og andre opphavere og for hvordan det kreative innholdet deres opprettes, distribueres, brukes og forbrukes. Utvikling og trening av slike modeller krever tilgang til store mengder tekst, bilder, video og andre data. Teknikker for tekst- og datautvinning kan brukes i stor utstrekning i denne sammenhengen til å innhente og analysere slikt innhold, som kan være beskyttet av opphavsrett og nærstående rettigheter. All bruk av opphavsrettsbeskyttet innhold krever tillatelse fra den berørte rettighetshaveren med mindre relevante opphavsrettslige unntak og begrensninger gjelder. Ved direktiv (EU) 2019/790 ble det innført unntak og avgrensinger som tillater eksemplarframstillinger av og uttrekk fra verk eller andre arbeider for tekst- og datautvinningsformål på visse vilkår. I henhold til disse reglene kan rettighetshaverne velge å forbeholde seg rettighetene til sine verk eller andre vernede arbeider for å hindre tekst- og datautvinning, med mindre denne utvinning- en gjøres med henblikk på vitenskapelig forskning. Dersom retten til unntak er blitt uttrykkelig forbeholdt på hensikts-

⁽⁴⁰⁾ Europaparlaments- og rådsdirektiv (EU) 2019/790 av 17. april 2019 om opphavsrett og nærstående 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).

messig måte, må leverandører av KI-modeller for allmenne formål innhente tillatelse fra rettighetshaverne dersom de ønsker å utføre tekst- og datautvinning fra slike verk.

- 106) Leverandører som bringer KI-modeller for allmenne formål i omsetning i Unionen, bør sikre at de relevante forpliktelsene i denne forordningen overholdes. For dette formålet bør leverandører av KI-modeller for allmenne formål innføre en framgangsmåte for å overholde unionsretten om opphavsrett og nærstående rettigheter, særlig for å identifisere og etterleve rettighetshaveres forbeholdelse av rettigheter i samsvar med artikkel 4 nr. 3 i direktiv (EU) 2019/790. Enhver leverandør som bringer en KI-modell for allmenne formål i omsetning i Unionen, bør oppfylle denne forpliktelsen, uavhengig av i hvilken jurisdiksjon de opphavsrettslig relevante handlingene som ligger til grunn for treningen av disse KI-modellene, finner sted. Dette er nødvendig for å sikre like vilkår for leverandører av KI-modeller for allmenne formål, der ingen leverandør bør kunne oppnå et konkurransefortrinn på unionsmarkedet ved å anvende lavere opphavsrettsstandarder enn de som er fastsatt i Unionen.
- 107) For å øke åpenheten om dataene som brukes i forhåndstrening og trening av KI-modeller for allmenne formål, herunder tekst og data som er beskyttet av opphavsrett, er det tilstrekkelig at leverandører av slike modeller utarbeider og offentliggjør et tilstrekkelig detaljert sammendrag av innholdet som brukes til treningen av KI-modellen for allmenne formål. Samtidig som det tas behørig hensyn til behovet for å beskytte forretningshemmeligheter og fortrolig forretningsinformasjon, bør innholdet i dette sammendraget være bredt anlagt i stedet for teknisk detaljert, for å bidra til at parter med berettiget interesse, herunder rettighetshaverne, kan utøve og håndheve sine rettigheter i henhold til unionsretten, for eksempel ved å liste opp de viktigste datasamlingene eller datasettene som er brukt til å trene modellen, så som store private eller offentlige databaser eller dataarkiver, og ved å gi en beskrivende redegjørelse for andre datakilder som er brukt. KI-kontoret bør stille til rådighet en mal for sammendraget som bør være enkel og effektiv, og som bør gjøre det mulig for leverandøren å gi det påkrevde sammendraget i beskrivende form.
- 108) Når det gjelder forpliktelsene som leverandører av KI-modeller for allmenne formål har til å innføre en framgangsmåte for å overholde unionsretten om Unionens opphavsretsregler og offentliggjøre et sammendrag av innholdet som er brukt til treningen, bør KI-kontoret overvåke om leverandøren har oppfylt disse forpliktelsene, uten å verifisere eller gå videre til en vurdering av treningsdataene verk for verk med hensyn til overholdelse av opphavsretten. Denne forordningen berører ikke håndhevelsen av opphavsretsreglene som fastsatt i unionsretten.
- 109) Overholdelsen av forpliktelsene som gjelder for leverandører av KI-modeller for allmenne formål, bør stå i forhold til typen modelleverandør, noe som innebærer at personer som utvikler eller bruker modellene for ikke-yrkesmessige formål eller med henblikk på vitenskapelig forskning, ikke er pålagt å overholde disse kravene, men de bør likevel oppfordres til å overholde dem frivillig. Uten at det berører Unionens opphavsretsregler, bør det i forbindelse med overholdelsen av disse forpliktelsene tas behørig hensyn til leverandørens størrelse, og det bør finnes forenklede måter å overholde forpliktelsene på for små og mellomstore bedrifter, herunder oppstartsbedrifter, som ikke bør innebære en urimelig kostnad og ikke motvirke bruk av slike modeller. Ved endring eller finjustering av en modell bør forpliktelsene for leverandører av KI-modeller for allmenne formål begrenses til denne endringen eller finjusteringen, for eksempel ved å supplere den allerede eksisterende tekniske dokumentasjonen med informasjon om endringene, herunder nye treningsdatakilder, som en måte å overholde verdikjedeforpliktelsene fastsatt i denne forordningen på.
- 110) KI-modeller for allmenne formål kan innebære systemrisiko som omfatter, men ikke er begrenset til, faktiske eller rimelig forutsigbare negative virkninger i forbindelse med større ulykker, forstyrrelser i kritiske sektorer og alvorlige konsekvenser for folkehelsen og offentlig sikkerhet, faktiske eller rimelig forutsigbare negative virkninger på demokratiske prosesser, offentlig og økonomisk sikkerhet og spredning av ulovlig, falskt eller diskriminerende innhold. Det bør antas at systemrisikoen øker i takt med modellens kapasitet og rekkevidde, kan oppstå gjennom hele modellens livssyklus og påvirkes av forhold med feilbruk, modellens pålitelighet, rettferdighet, sikkerhet, grad av autonomi og dens tilgang til verktøy, nye eller kombinerte metoder, strategier for frigivelse og distribusjon, potensialet til å fjerne beskyttelsesmekanismer og andre faktorer. Særlig har internasjonale tilnærminger hittil påvist behovet for å være oppmerksom på risiko som følge av potensiell bevisst feilbruk eller utilsiktede problemer med kontroll i forbindelse med tilpasning til mennes-

kelig hensikt; kjemisk, biologisk, radiologisk og kjernefysisk risiko, for eksempel hvordan adgangsbarrierer kan reduseres, herunder for utvikling, anskaffelse eller bruk av våpen; offensiv cyberkapasitet, for eksempel hvordan avdekking, utnyttelse eller operativ bruk av sårbarheter kan muliggjøres; virkningene av samhandling og verktøybruk, herunder for eksempel kapasitet til å kontrollere fysiske systemer og forstyrre kritisk infrastruktur; risiko for at modeller kan lage kopier av seg selv eller «selvreplikere» eller trene andre modeller; hvordan modellene kan forårsake skadelige skjevheter og diskriminering med risiko for enkeltpersoner, fellesskap eller samfunn; tilrettelegging for desinformasjon eller sveiking av personvernet med trusler mot demokratiske verdier og menneskerettigheter; risiko for at en bestemt hendelse kan føre til en kjedereaksjon med betydelige negative virkninger som vil kunne påvirke opptil en hel by, en hel virksomhetssektor eller et helt fellesskap.

- 111) Det bør utarbeides en metode for klassifisering av KI-modeller for allmenne formål som KI-modeller for allmenne formål med systemrisiko. Ettersom systemrisikoen skyldes særlig sterke kapabiliteter, bør en KI-modell for allmenne formål anses å utgjøre en systemrisiko dersom den har kapabiliteter med høy påvirkningsgrad, vurdert på grunnlag av egnede tekniske verktøy og metoder, eller har betydelig innvirkning på det indre marked på grunn av sin rekkevidde. Kapabiliteter med høy påvirkningsgrad i KI-modeller for allmenne formål er kapabiliteter som svarer til eller overgår de kapabilitetene som er registrert i de mest avanserte KI-modellene for allmenne formål. Det fullstendige utvalget av kapabiliteter i en modell vil kunne forstås bedre etter at den er brakt i omsetning, eller når idriftsettere samhandler med modellen. I henhold til det aktuelle tekniske utviklingstrinnet på tidspunktet for ikrafttreddelsen av denne forordningen er den samlede regnekraften som brukes til trening av KI-modellen for allmenne formål, målt i antall flyttallsoperasjoner, en av de relevante tilnærmingsverdiene for modellens kapabiliteter. Den samlede regnekraften som brukes til treningen, omfatter de regneoperasjonene som brukes på tvers av aktivitetene og metodene som har som formål å styrke modellens kapabiliteter før den settes i drift, for eksempel forhåndstrening, generering av syntetiske data og finjustering. Derfor bør det fastsettes en innledende terskel for antall flyttallsoperasjoner som, dersom en KI-modell for allmenne formål når denne terskelen, fører til en formodning om at modellen er en KI-modell for allmenne formål med systemrisiko. Denne terskelen bør justeres over tid for å gjenspeile teknologiske og industrielle endringer, for eksempel algoritmiske forbedringer eller mer effektiv maskinvare, og bør suppleres med referanseverdier og indikatorer for modellkapabilitet. For dette formålet bør KI-kontoret samarbeide med det vitenskapelige samfunnet, industrien, sivilsamfunnet og andre eksperter. Tersklene, i tillegg til verktøy og referanseverdier for vurdering av kapabiliteter med høy påvirkningsgrad, bør være sterke prediktorer for allmenngyldighet, kapabiliteter og tilhørende systemrisiko med hensyn til KI-modeller for allmenne formål, og kan ta høyde for hvordan modellen vil bli brakt i omsetning, eller hvor mange brukere den kan påvirke. For å utfylle dette systemet bør det være mulig for Kommisjonen å treffe individuelle beslutninger som utpeker en KI-modell for allmenne formål som en KI-modell for allmenne formål med systemrisiko, dersom det viser seg at modellen har kapabiliteter eller en innvirkning som svarer til det som fanges opp med den fastsatte terskelen. Denne beslutningen bør treffes på grunnlag av en samlet vurdering av kriteriene for utpeking av en KI-modell for allmenne formål med systemrisiko fastsatt i et vedlegg til denne forordningen, for eksempel kvaliteten eller størrelsen på treningsdatasettet, antallet virksomhets- og sluttbrukere, metodene for inn- og utdata, graden av autonomi og skalerbarhet, eller verktøyene den har tilgang til. Etter begrunnet anmodning fra en leverandør av en modell som er utpekt som en KI-modell for allmenne formål med systemrisiko, bør Kommisjonen ta hensyn til anmodningen og kan beslutte å foreta en ny vurdering for å fastslå om KI-modellen for allmenne formål fortsatt kan anses å medføre systemrisiko.
- 112) Dessuten må det fastsettes en nøyaktig prosedyre for klassifisering av KI-modeller for allmenne formål med systemrisiko. En KI-modell for allmenne formål som når den gjeldende terskelen for kapabiliteter med høy påvirkningsgrad, bør formodes å være en KI-modell for allmenne formål med systemrisiko. Leverandøren bør underrette KI-kontoret senest to uker etter at kravene er oppfylt, eller senest to uker etter at det blir kjent at en KI-modell for allmenne formål vil oppfylle kravene som fører til formodningen. Dette er spesielt relevant når det gjelder terskelen for flyttallsoperasjoner, fordi trening av KI-modeller for allmenne formål krever betydelig planlegging som omfatter forhåndstilddeling av data-behandlingsressurser, og leverandørene av KI-modeller for allmenne formål kan derfor allerede før treningen er fullført, vite om modellen vil nå terskelen. I forbindelse med denne underretningen bør leverandøren kunne dokumentere at en KI-modell for allmenne formål på grunn av sine særlige egenskaper unntaksvis ikke innebærer systemrisiko, og at den derfor ikke bør klassifiseres som en KI-modell for allmenne formål med systemrisiko. Denne informasjonen er verdifull, fordi KI-kontoret da vet på forhånd at KI-modeller for allmenne formål med systemrisiko vil bli brakt i omsetning, og fordi leverandørene på et tidlig tidspunkt kan begynne å samarbeide med KI-kontoret. Informasjonen er særlig viktig når det gjelder KI-modeller for allmenne formål som det er planlagt å utgi som åpen kildekode, ettersom det kan være vans-

keligere å treffe nødvendige tiltak for å sikre overholdelse av forpliktelsene fastsatt i denne forordningen etter at modellen er utgitt som åpen kildekode.

- 113) Dersom Kommisjonen blir kjent med at en KI-modell for allmenne formål oppfyller kravene for å bli klassifisert som KI-modell for allmenne formål med systemrisiko, som enten ikke har vært kjent tidligere, eller som den relevante leverandøren har unnlatt å underrette Kommisjonen om, bør Kommisjonen gis myndighet til å utpeke den som en slik. Gjennom et system med kvalifiserte varsler, som kommer i tillegg til KI-kontorets overvåkningsvirksomhet, bør det sikres at KI-kontoret mottar informasjon fra vitenskapsgruppen om KI-modeller for allmenne formål som muligens bør klassifiseres som KI-modeller for allmenne formål med systemrisiko.
- 114) Leverandøren av en KI-modell for allmenne formål som innebærer systemrisiko, bør i tillegg til de forpliktelsene som gjelder for leverandører av KI-modeller for allmenne formål, være underlagt forpliktelser som har som formål å påvise og begrense slik risiko og gi tilstrekkelig vern av cybersikkerheten, uavhengig av om den leveres som en frittstående modell eller innebygd i et KI-system eller et produkt. For at disse målene skal nås, bør denne forordningen pålegge leverandørene å foreta de nødvendige evalueringene av modellene, særlig før de bringes i omsetning for første gang, inkludert gjennomføring og dokumentasjon av testing av modellene for ondsinnet bruk, også gjennom intern eller uavhengig eksternt testing når det er hensiktsmessig. I tillegg bør leverandører av KI-modeller for allmenne formål med systemrisiko kontinuerlig vurdere og begrense systemrisiko, blant annet ved å innføre retningslinjer for risikostyring, for eksempel ansvarlighets- og forvaltningsprosesser, gjennomføre overvåking etter omsetning, treffe hensiktsmessige tiltak i hele modellens livssyklus og samarbeide med relevante aktører langs KI-verdikjeden.
- 115) Leverandører av KI-modeller for allmenne formål med systemrisiko bør vurdere og begrense mulig systemrisiko. Dersom utviklingen eller bruken av en KI-modell for allmenne formål som kan innebære systemrisiko, til tross for forsøk på å identifisere og forebygge slik risiko, forårsaker en alvorlig hendelse, bør leverandøren av modellen uten ugrunnet opphold følge opp hendelsen og rapportere all relevant informasjon og mulige korrigerende tiltak til Kommisjonen og de nasjonale vedkommende myndighetene. Dessuten bør leverandørene sørge for et tilstrekkelig vern av modellens cybersikkerhet og dens fysiske infrastruktur dersom det er relevant, gjennom hele modellens livssyklus. Cybersikkerhetsvern knyttet til systemrisiko i forbindelse med ondsinnet bruk eller angrep bør ta behørig hensyn til utilsiktet modellekkasje, uautoriserte utgivelser, omgåelse av sikkerhetstiltak og forsvar mot cyberangrep, uautorisert tilgang eller modelltyveri. Dette vernet kan lettes ved å sikre modellvekter, algoritmer, servere og datasett, for eksempel gjennom operasjonelle sikkerhetstiltak for informasjonssikkerhet, spesifikke retningslinjer for cybersikkerhet, tilstrekkelige tekniske og etablerte løsninger samt cybertilgangskontroll og fysisk tilgangskontroll, som er egnet for de relevante omstendighetene og risikoene som er involvert.
- 116) KI-kontoret bør oppmuntre til og legge til rette for utarbeiding, gjennomgang og tilpasning av regler for god praksis, idet det tas hensyn til internasjonale tilnærminger. Alle leverandører av KI-modeller for allmenne formål kan inviteres til å delta. For å sikre at reglene for god praksis gjenspeiler det aktuelle tekniske utviklingstrinnet og tar behørig hensyn til en rekke ulike perspektiver, bør KI-kontoret samarbeide med relevante nasjonale vedkommende myndigheter, og eventuelt kunne rådføre seg med sivilsamfunnsorganisasjoner og andre relevante berørte parter samt eksperter, herunder vitenskapsgruppen, om utarbeiding av slike regler. Reglene for god praksis bør omfatte forpliktelser for leverandører av KI-modeller for allmenne formål og KI-modeller for allmenne formål som innebærer systemrisiko. Når det gjelder systemrisiko, bør reglene for god praksis dessuten bidra til å fastsette en risikotaksonomi for typen og arten av systemrisikoer på unionsnivå, herunder kildene til dem. Reglene for god praksis bør også fokusere på spesifikke tiltak for risikovurdering og risikoreduksjon.
- 117) Reglene for god praksis bør utgjøre et sentralt verktøy for å sikre at leverandørene av KI-modeller for allmenne formål oppfyller sine forpliktelser i henhold til denne forordningen. Leverandører bør kunne vise til reglene for god praksis for å dokumentere at de overholder forpliktelsene. Ved hjelp av gjennomføringsrettsakter kan Kommisjonen beslutte å god-

kjenne regler for god praksis og gi dem allmenn gyldighet i Unionen, eller alternativt å fastsette felles regler for gjennomføring av de relevante forpliktelsene, dersom reglene for god praksis på det tidspunktet denne forordningen får anvendelse, ikke kan ferdigstilles eller ikke anses tilstrekkelige av KI-kontoret. Så snart en harmonisert standard er offentliggjort og vurdert av KI-kontoret som egnet til å dekke de relevante forpliktelsene, bør leverandører som overholder en europeisk harmonisert standard, omfattes av formodningen om samsvar. Leverandører av KI-modeller for allmenne formål bør dessuten kunne dokumentere overholdelse med andre egnede midler dersom det ikke foreligger regler for god praksis eller harmoniserte standarder, eller dersom de velger å ikke vise til disse.

- 118) Denne forordningen regulerer KI-systemer og KI-modeller ved å fastsette 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 integrerer slike systemer eller modeller i sine tjenester, som er regulert av forordning (EU) 2022/2065. I den grad slike systemer eller modeller er integrert i utpekte svært store internettplattformer eller svært store nettbaserte søkemotorer, er de underlagt rammen for risikostyring fastsatt i forordning (EU) 2022/2065. Følgelig bør de tilsvarende forpliktelsene i denne forordningen formodes å være overholdt med mindre betydelig systemrisiko som ikke omfattes av forordning (EU) 2022/2065, oppstår og påvises i slike modeller. Innenfor denne rammen er tilbydere av svært store internettplattformer og svært store nettbaserte søkemotorer forpliktet til å vurdere potensiell systemrisiko som stammer fra utformingen, driften og bruken av deres tjenester, herunder hvordan utformingen av algoritmesystemer som brukes i tjenesten, kan bidra til slik risiko, samt systemrisiko som stammer fra potensiell feilbruk. Disse leverandørene er også forpliktet til å treffe egnede avbøtende tiltak for å overholde grunnleggende rettigheter.
- 119) I betraktning av den raske innovasjonstakten og den teknologiske utviklingen av digitale tjenester som omfattes av ulike EU-rettslige instrumenter, særlig med tanke på bruken av tjenestene og tjenestemottakernes oppfatning, kan de KI-systemene som omfattes av denne forordningen, leveres som formidlingstjenester som definert i forordning (EU) 2022/2065, eller deler av slike, som bør tolkes på en teknologinøytral måte. For eksempel kan KI-systemer brukes til å levere nettbaserte søkemotorer, særlig i den grad et KI-system, eksempelvis en nettbasert chatbot, søker på i prinsippet alle nettstedene, innarbeider resultatene i sin eksisterende kunnskap og bruker den oppdaterte kunnskapen til å generere ett sett med utdata som kombinerer informasjon fra ulike kilder.
- 120) Videre er forpliktelser som pålegges leverandører og idriftsettere av visse KI-systemer i denne forordningen for å gjøre det mulig å oppdage og opplyse om at utdata 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 den plikten tilbydere av svært store internettplattformer eller svært store nettbaserte søkemotorer har til å identifisere og begrense systemrisiko som kan oppstå ved spredning av kunstig generert eller manipulert innhold, særlig risiko for faktisk eller forutsigbar negativ innvirkning på demokratiske prosesser, samfunnsdebatten og valgprosesser, herunder gjennom desinformasjon.
- 121) Standardisering bør spille en nøkkelrolle når det gjelder å gi leverandørene tekniske løsninger som sikrer at denne forordningen overholdes, i samsvar med det aktuelle tekniske utviklingstrinnet, for å fremme innovasjon, konkurranseevne og vekst i det indre marked. Overholdelse av harmoniserte standarder som definert i artikkel 2 nr. 1 bokstav c) i europaparlaments- og rådsforordning (EU) nr. 1025/2012⁽⁴¹⁾, som normalt forventes å gjenspeile det aktuelle tekniske utviklingstrinnet, bør være et middel for leverandørene til å dokumentere at kravene i denne forordningen er oppfylt. Det bør derfor oppmuntres til en balansert representasjon av interesser ved utarbeidingen av standarder som involverer alle relevante berørte parter, særlig SMB-er, forbruker- og miljøorganisasjoner og sosiale interessenter, i samsvar med artikkel 5 og 6 i forordning (EU) nr. 1025/2012. For å lette overholdelsen bør Kommisjonen utstede anmodningene om standardisering uten unødig opphold. Ved utarbeidingen av anmodningen om standardisering bør Kommisjonen rådføre seg med det rådgivende forumet og KI-rådet for å innhente relevant ekspertise. Dersom det ikke finnes relevante henvisninger til harmoniserte standarder, bør Kommisjonen imidlertid, via gjennomføringsrettsakter og etter å ha rådført seg med det rådgivende forumet, kunne fastsette felles spesifikasjoner for visse krav som følger av denne forordningen. Den felles spesifikasjonen bør være en unntaksløsning for å lette leverandørens plikt til å oppfylle kravene i denne forordningen,

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

når anmodningen om standardisering ikke er blitt godtatt av noen av de europeiske standardiseringsorganisasjonene, når de relevante harmoniserte standardene ikke tar tilstrekkelig hensyn til spørsmål knyttet til grunnleggende rettigheter eller ikke er i samsvar med anmodningen, eller når vedtakelsen av en egnet harmonisert standard er forsinket. Dersom en slik forsinkelse i vedtakelsen av en harmonisert standard skyldes standardens tekniske kompleksitet, bør dette vurderes av Kommisjonen før det overveies å fastsette felles spesifikasjoner. Ved utarbeidingen av felles spesifikasjoner oppmuntres Kommisjonen til å samarbeide med internasjonale partnere og internasjonale standardiseringsorganer.

- 122) Uten at det berører bruken av harmoniserte standarder og felles spesifikasjoner, bør leverandører av KI-systemer med høy risiko som er trent og testet på data som avspeiler de særskilte geografiske, atferdsmessige, kontekstuelle eller funksjonelle omgivelsene der KI-systemet er ment å brukes, formodes å være i samsvar med det relevante tiltaket som er fastsatt i henhold til kravet om dataforvaltning i denne forordningen. I samsvar med artikkel 54 nr. 3 i forordning (EU) 2019/881 bør KI-systemer med høy risiko som er sertifisert eller som det er utstedt en samsvarserklæring for i henhold til en cybersikkerhetsordning i samsvar med nevnte forordning, og som det er offentliggjort henvisninger til i *Den europeiske unions tidende*, uten at det berører kravene til robusthet og nøyaktighet fastsatt i denne forordningen, formodes å oppfylle cybersikkerhetskravet i denne forordningen i det omfanget cybersikkerhetssertifikatet eller samsvarserklæringen eller deler av disse dekker cybersikkerhetskravet i denne forordningen. Dette berører ikke cybersikkerhetsordningens frivillige karakter.
- 123) For å sikre at KI-systemer med høy risiko har høy grad av pålitelighet, bør disse systemene gjennomgå en samsvarsvurdering før de bringes i omsetning eller tas i bruk.
- 124) For å minimere byrden for operatørene og unngå dobbeltarbeid bør vurderingen av om KI-systemer med høy risiko som er knyttet til produkter som omfattes av eksisterende EU-harmoniseringsregelverk basert på den nye rettslige rammen, er i samsvar med kravene i denne forordningen, foretas som en del av den samsvarsvurderingen som allerede er fastsatt i nevnte regelverk. Om kravene i denne forordningen får anvendelse eller ikke, bør derfor ikke påvirke den spesifikke logikken, metodikken eller generelle strukturen til den samsvarsvurderingen som er fastsatt i det relevante EU-harmoniseringsregelverket.
- 125) På grunn av kompleksiteten til KI-systemer med høy risiko og risikoen forbundet med dem er det viktig å utarbeide en hensiktsmessig prosedyre for samsvarsvurdering av slike systemer som involverer meldte organer, såkalt tredjeparts samsvarsvurdering. På bakgrunn av de nåværende erfaringene til profesjonelle organer som utfører sertifisering før omsetning på området produktsikkerhet, og forskjellen i hvilken risiko som er involvert, er det imidlertid hensiktsmessig, i det minste i en innledende fase av anvendelsen av denne forordningen, å begrense anvendelsesområdet for tredjeparts samsvarsvurdering når det gjelder andre KI-systemer med høy risiko enn dem som er knyttet til produkter. Samsvarsvurderingen av slike systemer bør derfor som hovedregel utføres av leverandøren på dennes eget ansvar, idet det eneste unntaket bør være KI-systemer som er beregnet på å brukes til biometri.
- 126) For å kunne utføre tredjeparts samsvarsvurdering når det er påkrevd, bør meldte organer meldes av de nasjonale vedkommende myndighetene i henhold til denne forordningen, forutsatt at organene oppfyller et sett med krav, særlig krav om uavhengighet, kompetanse og fravær av interessekonflikter samt egnede cybersikkerhetskrav. Disse organene bør meldes av nasjonale vedkommende myndigheter til Kommisjonen og de andre medlemsstatene ved hjelp av det elektroniske meldingsverktøyet som Kommisjonen har utviklet og forvalter 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 handelshindringer er det hensiktsmessig å lette den gjensidige anerkjennelsen av samsvarsvurderingsresultater fra kompetente samsvarsvurderingsorganer, uavhengig av på hvilket territorium de er etablert, forutsatt at de samsvarsvurderingsorganene som er opprettet i henhold til et tredjelandets rett, oppfyller de gjeldende kravene i denne forordningen, og at Unionen har inngått en avtale om dette. I denne sammenhengen bør Kommisjonen aktivt undersøke mulige internasjonale instrumenter for dette formålet og særlig søke å inngå avtaler om gjensidig anerkjennelse med tredjeland.
- 128) I tråd med det allment etablerte begrepet «vesentlig endring» for produkter som reguleres av EU-harmoniseringsregelverk, er det hensiktsmessig at når det skjer en endring som kan påvirke i hvilken grad et KI-system med høy risiko er i samsvar med denne forordningen (for eksempel bytte av operativsystem eller programvarearkitektur), eller når systemets tiltenkte formål endres, så anses dette KI-systemet som et nytt KI-system som bør underkastes en ny samsvarsvurdering. Derimot bør endringer i algoritmen og ytelsen til KI-systemer som fortsetter å «lære» etter at de er brakt i omsetning eller tatt i bruk, det vil si at de automatisk tilpasser måten funksjoner utføres på, ikke utgjøre vesentlige endringer, forutsatt at disse endringene er forhåndsbestemt av leverandøren og vurdert på tidspunktet for samsvarsvurderingen.

- 129) KI-systemer med høy risiko bør ha CE-merking som viser at de er i samsvar med denne forordningen, slik at de fritt kan omsettes på det indre marked. For KI-systemer med høy risiko som er innebygd i et produkt, bør det påføres en fysisk CE-merking, og denne kan suppleres med en digital CE-merking. For KI-systemer med høy risiko som bare leveres digitalt, bør det brukes en digital CE-merking. Medlemsstatene bør ikke skape uberettigede hindringer for å bringe i omsetning eller ta i bruk KI-systemer med høy risiko som oppfyller kravene i denne forordningen og bærer CE-merkingen.
- 130) Under visse omstendigheter kan det være avgjørende for menneskers helse og sikkerhet, for miljøvern og klimaendringer og for samfunnet som helhet at nyskapende teknologi blir tilgjengelig raskt. 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 viktig industri og infrastruktur, kan tillate at KI-systemer som ikke har gjennomgått en samsvarsvurdering, bringes i omsetning eller tas i bruk. I behørig begrunnede tilfeller, som fastsatt i denne forordningen, kan de rettshåndhevende myndighetene eller myndighetene for sivil beredskap ta i bruk et bestemt KI-system med høy risiko uten tillatelse fra markedstilsynsmyndigheten, forutsatt at det søkes slik tillatelse uten ugrunnet opphold under eller etter bruken.
- 131) For å lette Kommisjonens og medlemsstatenes arbeid på KI-området og øke åpenheten overfor allmennheten bør andre leverandører av KI-systemer med høy risiko enn dem som er knyttet til produkter omfattet av relevant eksisterende EU-harmoniseringsregelverk, samt leverandører som anser at et KI-system som er oppført blant brukstilfellene med høy risiko i et vedlegg til denne forordningen, på grunnlag av et unntak ikke innebærer høy risiko, være pålagt å registrere informasjon om seg selv og sitt KI-system i en EU-database som skal opprettes og forvaltes av Kommisjonen. Før de bruker et KI-system som er oppført blant brukstilfellene med høy risiko i et vedlegg til denne forordningen, bør idriftsettere av KI-systemer med høy risiko som er offentlige myndigheter, byråer eller organer, registrere seg i denne databasen og velge det systemet de har til hensikt å bruke. Andre idriftsettere bør ha rett til å gjøre dette frivillig. Denne delen av EU-databasen bør være offentlig og kostnadsfritt tilgjengelig, og informasjonen bør være lett å navigere i, forståelig og maskinlesbar. EU-databasen bør også være brukervennlig, for eksempel ved at den har søkefunksjoner, herunder nøkkelordsøk, som gjør det mulig for allmennheten å finne relevant informasjon som skal oppgis ved registrering av KI-systemer med høy risiko, og om hvilket brukstilfelle av KI-systemer med høy risiko, som angitt i et vedlegg til denne forordningen, som KI-systemene med høy risiko svarer til. Alle vesentlige endringer av KI-systemer med høy risiko bør også registreres i EU-databasen. For KI-systemer med høy risiko på områdene rettshåndhevelse og migrasjons-, 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 når det gjelder deres nasjonale del av databasen. KI-systemer med høy risiko på området kritisk infrastruktur bør bare registreres på nasjonalt plan. 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 settes i drift, bør prosedyren for å opprette databasen omfatte funksjonsspesifikasjoner som utarbeides av Kommisjonen, og en uavhengig revisjonsrapport. Kommisjonen bør ta hensyn til cybersikkerhetsrisiko når den utfører sine oppgaver som behandlingsansvarlig for EU-databasen. For å maksimere tilgjengeligheten og allmennhetens bruk av EU-databasen bør både databasen og de opplysningene som gjøres tilgjengelige ved hjelp av den, oppfylle kravene i direktiv (EU) 2019/882.
- 132) Visse KI-systemer som er beregnet på å samhandle med fysiske personer eller å generere innhold, kan utgjøre en særskilt risiko for identitetstyveri eller bedrageri, uansett om de anses for å ha høy risiko eller ikke. Under visse omstendigheter bør bruken av disse systemene derfor være underlagt særlige forpliktelser om åpenhet, uten at det berører kravene og forpliktelsene i forbindelse med KI-systemer med høy risiko, og med forbehold om målrettede unntak for å ta hensyn til de særlige behovene innenfor rettshåndhevelse. Særlig bør fysiske personer varsles om at de samhandler med et KI-system, med mindre dette er åpenbart for en fysisk person som er rimelig velinformert, observant og aktsom, tatt i betraktning omstendighetene og brukskonteksten. Ved gjennomføringen av denne forpliktelsen bør det tas hensyn til egenkapene til fysiske personer som på grunn av alder eller funksjonsnedsettelse tilhører sårbare grupper, i den grad KI-systemet er beregnet på å samhandle også med disse gruppene. Dessuten bør fysiske personer varsles når de eksponeres for KI-systemer som ved at de behandler deres biometriske opplysninger, kan identifisere eller utlede disse personenes følelser eller intensjoner eller plassere dem i bestemte kategorier. Slike kategorier kan ha sammenheng med kjennetegn som kjønn, alder, hårfarge, øyenfarge, tatoveringer, personlighetstrekk, etnisk opprinnelse, personlige preferanser og interesser. Slik informasjon og slike varsler bør gis i et format som er tilgjengelig for personer med funksjonsnedsettelse.

- 133) En rekke KI-systemer kan generere store mengder syntetisk innhold som blir stadig vanskeligere for mennesker å skille fra menneskelig generert og autentisk innhold. Den brede tilgjengeligheten og de økende kapabilitetene til disse systemene har en betydelig innvirkning på integriteten og tilliten til informasjonsøkosystemet, noe som skaper ny risiko for feilinformasjon og manipulering i stor skala, bedrageri, identitetstyveri og villedning av forbrukerne. På bakgrunn av disse konsekvensene, den raske teknologiske utviklingen og behovet for nye metoder og teknikker for å spore informasjonen tilbake til opprinnelsen, bør leverandørene av disse systemene bygge inn tekniske løsninger som gjør det mulig å merke utdataene i et maskinlesbart format med at de er generert eller manipulert av et KI-system og ikke et menneske, og å påvise at de er det. Slike teknikker og metoder bør være så pålitelige, samvirkende, effektive og robuste som teknisk mulig, tatt i betraktning de tilgjengelige teknikkene eller en kombinasjon av slike teknikker, for eksempel vannmerker, identifikasjon av metadata, kryptografiske metoder for å bevise innholdets opprinnelse og ekthet, loggingsmetoder, fingeravtrykk eller andre teknikker, alt etter hva som er hensiktsmessig. Ved gjennomføringen av denne forpliktelsen bør leverandørene også ta hensyn til særtrekkene og begrensningene ved de ulike innholdstypene og den relevante teknologiske utviklingen og markedsutviklingen på området, slik som dette gjenspeiles i det allment anerkjente aktuelle tekniske utviklingstrinnet. Slike teknikker og metoder kan innføres på KI-systemnivå eller KI-modellnivå, herunder i KI-modeller for allmenne formål som genererer innhold, for på den måten å gjøre det lettere for nedstrømsleverandøren av KI-systemet å oppfylle denne forpliktelsen. For at den skal være forholdsmessig, bør denne merkingsplikten ikke gjelde KI-systemer som primært utfører en hjelpefunksjon for standardredigering, eller KI-systemer som ikke i vesentlig grad endrer inndataene fra idriftsetteren eller semantikken i disse.
- 134) I tillegg til de tekniske løsningene som brukes av leverandørene av KI-systemet, bør idriftsettere som bruker et KI-system til å generere eller manipulere bilde-, lyd- eller videoinnhold som i vesentlig grad ligner eksisterende personer, gjenstander, steder, enheter eller hendelser, og som feilaktig framstår for en person som autentisk eller sannferdig (dypforfalskning), klart og tydelig opplyse om at innholdet er kunstig skapt eller manipulert, ved å merke KI-utdataene i samsvar med dette og oppgi den kunstige opprinnelsen. Overholdelse av denne plikten til åpenhet bør ikke tolkes som en indikasjon på at bruk av KI-systemet eller dets utdata hindrer retten til ytringsfrihet eller retten til frihet for kunst og vitenskap som er garantert i pakten, særlig ikke dersom innholdet inngår i et åpenbart kreativt, satirisk, kunstnerisk, fiktivt eller tilsvarende verk eller program, med forbehold om tilstrekkelige garantier for tredjeparters rettigheter og friheter. I slike tilfeller er plikten til åpenhet om dypforfalskninger som er fastsatt i denne forordningen, begrenset til å opplyse om at slikt generert eller manipulert innhold forekommer, på en hensiktsmessig måte som ikke hindrer at verket vises fram eller nyttes, inkludert normal utnyttelse og bruk av det, samtidig som verkets nytteverdi og kvalitet opprettholdes. Det bør også innføres en lignende opplysningsplikt i forbindelse med KI-genererte eller -manipulerte tekster dersom de offentliggjøres for å informere allmennheten om saker av allmenn interesse, med mindre det KI-genererte innholdet er gjennomgått av mennesker eller har vært gjenstand for redaksjonell kontroll, og en fysisk eller juridisk person har redaksjonelt ansvar for offentliggjøringen av innholdet.
- 135) Uten at det berører det faktum at plikten til åpenhet er obligatorisk og gjelder fullt ut, kan Kommissjonen også oppmuntre til og legge til rette for at det utarbeides regler for god praksis på unionsplan med tanke på å lette effektiv gjennomføring av forpliktelsene om påvisning og merking av kunstig generert eller manipulert innhold, herunder, dersom det er relevant, som grunnlag for de praktiske ordningene for å gjøre påvisningsmekanismene tilgjengelige og for å lette samarbeidet med andre aktører i verdikjeden, spre innhold eller kontrollere innholdets ekthet og opprinnelse, slik at allmennheten effektivt kan skille KI-generert innhold fra annet innhold.
- 136) Forpliktelsene som pålegges leverandører og idriftsettere av visse KI-systemer i denne forordningen for å gjøre det mulig å oppdage og opplyse om at utdata 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 den plikten tilbydere av svært store internettplattformer eller svært store nettbaserte søkemotorer har til å identifisere og begrense systemrisiko som kan oppstå ved spredning av kunstig generert eller manipulert innhold, særlig risiko for faktisk eller forutsigbar negativ innvirkning på demokratiske prosesser, samfunnsdebatten og valgprosesser, herunder gjennom desinformasjon. Denne forordningens krav om å merke innhold som er generert av KI-systemer, berører ikke den plikten som tilbydere av vertstjenester har i henhold til artikkel 16 nr. 6 i forordning (EU) 2022/2065 til å behandle meldinger om ulovlig innhold som mottas i samsvar med artikkel 16 nr. 1 i samme forordning, og bør ikke påvirke vurderingen av og beslutningen om hvorvidt det spesifikke innholdet er ulovlig. Denne vurderingen bør gjøres utelukkende på grunnlag av de reglene som regulerer lovligheten av innholdet.

- 137) Overholdelse av plikten til åpenhet om de KI-systemene som omfattes av denne forordningen, bør ikke tolkes som en indikasjon på at bruk av KI-systemet eller dets utdata er lovlig i henhold til denne forordningen eller annen unionsrett eller medlemsstatenes rett, og bør ikke berøre andre åpenhetsforpliktelser for idriftsettere som er fastsatt i unionsretten eller nasjonal rett.
- 138) KI er en familie av teknologier i rask utvikling som krever regulatorisk tilsyn og et trygt og kontrollert rom for eksperimentering, samtidig som det sikres ansvarlig innovasjon og integrering av hensiktsmessige sikkerhetstiltak og risikoreduserende tiltak. For å sikre en rettslig ramme som fremmer innovasjon og er framtidssikret og motstandsdyktig mot forstyrrelser, bør medlemsstatene sikre at deres nasjonale vedkommende myndigheter oppretter minst én regulatorisk sandkasse for KI på nasjonalt plan for å lette utviklingen og testingen av innovative KI-systemer under strengt regulatorisk tilsyn før systemene bringes i omsetning eller tas i bruk på annen måte. Medlemsstatene kan også oppfylle denne forpliktelsen ved å delta i allerede eksisterende regulatoriske sandkasser eller ved å opprette en sandkasse sammen med en eller flere medlemsstaters vedkommende myndigheter, i den grad denne deltakelsen gir tilsvarende grad av nasjonal dekning for de deltagende medlemsstatene. Regulatoriske sandkasser for KI kan opprettes i fysisk, digital eller hybrid form og kan romme både fysiske og digitale produkter. Myndighetene som oppretter dem, bør også sikre at de regulatoriske sandkassene for KI har tilstrekkelige ressurser til at de kan fungere, herunder økonomiske og menneskelige ressurser.
- 139) Målene med de regulatoriske sandkassene for KI bør være å fremme KI-innovasjon ved å opprette et kontrollert miljø for eksperimentering og testing i utviklingsfasen og fasen før omsetning, med sikte på å sørge for at de nyskapende KI-systemene er i samsvar med denne forordningen og annen relevant unionsrett og nasjonal rett. Videre bør de regulatoriske sandkassene for KI ha som mål å styrke den rettslige forutsigbarheten for innovatører samt vedkommende myndigheters tilsyn med og forståelse av mulighetene, de framvoksende risikoene ved og virkningene av KI-bruk, å legge til rette for regulatorisk læring for myndigheter og foretak, blant annet med tanke 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 KI, og å gi raskere markedstilgang, blant annet ved å fjerne hindringer for små og mellomstore bedrifter, herunder oppstartsbedrifter. Regulatoriske sandkasser for KI bør være vidt tilgjengelige i hele Unionen, og det bør legges særlig vekt på at de er tilgjengelige for små og mellomstore bedrifter, herunder oppstartsbedrifter. Deltakelsen i den regulatoriske sandkassen for KI bør fokusere på forhold som skaper rettslig usikkerhet for leverandører og prospektive leverandører, med sikte på å drive nyskaping, prøve ut KI i Unionen og bidra til evidensbasert regulatorisk læring. Tilsynet med KI-systemene i den regulatoriske sandkassen for KI bør derfor omfatte utvikling, trening, testing og validering av KI-systemene før de bringes i omsetning eller tas i bruk, samt begrepet vesentlig endring og forekomst av vesentlige endringer som kan kreve en ny prosedyre for samsvarsvurdering. Dersom det avdekkes betydelig risiko under utviklingen og testingen av slike KI-systemer, bør det treffes egnede risikoreduserende tiltak og, dersom dette ikke er mulig, bør utviklings- og testprosessen stoppes. Når det er hensiktsmessig, bør nasjonale vedkommende myndigheter som oppretter regulatoriske sandkasser for KI, samarbeide med andre relevante myndigheter, herunder de som fører tilsyn med vernet av grunnleggende rettigheter, og kan gi rom for deltakelse fra andre aktører innenfor KI-økosystemet, for eksempel nasjonale eller europeiske standardiseringsorganisasjoner, meldte organer, test- og forsøksanlegg, forsknings- og forsøkslaboratorier, europeiske digitale innovasjonsnav og relevante interesse- og sivilsamfunnsorganisasjoner. For å sikre lik gjennomføring i hele Unionen og stordriftsfordeler bør det fastsettes felles regler for gjennomføringen av de regulatoriske sandkassene for KI og et rammeverk for samarbeid mellom de relevante myndighetene som deltar i tilsynet med sandkassene. Regulatoriske sandkasser for KI som er opprettet i samsvar med denne forordningen, bør ikke berøre annen rett som åpner for at det opprettes andre sandkasser for å sikre samsvar med annet regelverk enn denne forordningen. Når det er hensiktsmessig, bør de relevante vedkommende myndighetene som har ansvar for disse andre regulatoriske sandkassene, vurdere fordelene ved å bruke dem også for å sikre at KI-systemene er i samsvar med denne forordningen. Etter avtale mellom de nasjonale vedkommende myndighetene og deltakerne i den regulatoriske sandkassen for KI, kan testing under virkelige forhold også gjennomføres og overvåkes innenfor rammen av den regulatoriske sandkassen for KI.
- 140) Denne forordningen bør utgjøre det rettslige grunnlaget for at leverandørene og de prospektive leverandørene i den regulatoriske sandkassen for KI kan bruke personopplysninger som samles inn for andre formål, til 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 forblir gjeldende. Særlig bør ikke denne forordningen danne rettslig grunnlag i henhold til artik-

kel 22 nr. 2 bokstav b) i forordning (EU) 2016/679 og artikkel 24 nr. 2 bokstav b) i forordning (EU) 2018/1725. Leverandører og prospektive leverandører i den regulatoriske sandkassen for KI bør sørge for hensiktsmessige sikkerhetstiltak og samarbeide med vedkommende myndigheter, blant annet ved å følge veiledning fra dem og handle raskt og i god tro for å redusere all påvist betydelig risiko for sikkerhet, helse og grunnleggende rettigheter som kan oppstå under utvikling, testing og eksperimentering i sandkassen.

- 141) For å framskynde utviklingsprosessen for de KI-systemene med høy risiko som er oppført i et vedlegg til denne forordningen, og for at de raskere skal kunne bringes i omsetning, er det viktig at leverandører eller prospektive leverandører av slike systemer også kan dra nytte av en spesifikk ordning for testing av disse systemene under virkelige forhold, uten å delta i en regulatorisk sandkasse for KI. I slike tilfeller bør det imidlertid, samtidig som det tas hensyn til de mulige konsekvensene av slike tester for enkeltpersoner, sikres at det innføres hensiktsmessige og tilstrekkelige garantier og vilkår for leverandører eller prospektive leverandører ved denne forordningen. Slike garantier bør omfatte blant annet å be om informert samtykke fra fysiske personer til å delta i testing under virkelige forhold, med unntak av rettshåndhevelse der det å søke informert samtykke ville hindre KI-systemet i å bli testet. Samtykke fra forsøkspersoner til å delta i slik testing i henhold til denne forordningen skiller seg fra, og berører ikke, samtykke fra registrerte til behandling av deres personopplysninger i henhold til den relevante retten om vern av personopplysninger. Det er også viktig å minimere risikoen og muliggjøre tilsyn fra vedkommende myndigheter og derfor å pålegge prospektive leverandører å ha en plan for testing under virkelige forhold som oversendes vedkommende markedstilsynsmyndighet, med visse begrensede unntak å registrere testingen i særskilte deler av EU-databasen – med visse begrensede unntak, å avgrense perioden da testingen kan gjennomføres, og å kreve ytterligere sikkerhetstiltak for personer som tilhører visse sårbare grupper, samt å ha en skriftlig avtale som fastsetter rollen og ansvaret til prospektive leverandører og idriftsettere og effektivt tilsyn av kompetent personell som deltar i testingen under virkelige forhold. Dessuten bør det fastsettes ytterligere sikkerhetstiltak for å sikre at KI-systemets prediksjoner, anbefalinger eller beslutninger effektivt kan reverseres og ignorerer, og at personopplysninger blir beskyttet og blir slettet når forsøkspersonene har trukket tilbake samtykket til å delta i testingen, uten at det berører deres rettigheter som registrerte i henhold til unionsretten om vern av personopplysninger. Når det gjelder overføring av data, bør det også fastsettes at data som samles inn og behandles i forbindelse med testing under virkelige forhold, bare bør overføres til tredjeland dersom det er innført hensiktsmessige og gjeldende sikkerhetstiltak i henhold til unionsretten, særlig i samsvar med de forutsetningene for å overføre personopplysninger som følger av unionsretten om vern av personopplysninger, mens det for ikke-personopplysninger er innført egnede sikkerhetstiltak i samsvar med unionsretten, så som europaparlaments- og rådsforordning (EU) 2022/868⁽⁴²⁾ og (EU) 2023/2854⁽⁴³⁾.
- 142) For å sikre at KI fører til sosialt og miljømessig gunstige resultater, oppfordres medlemsstatene til å støtte og fremme forskning på og utvikling av KI-løsninger til støtte for sosialt og miljømessig gunstige resultater, for eksempel KI-baserte løsninger for å øke tilgjengeligheten for personer med funksjonsnedsettelse, takle sosioøkonomiske ulikheter eller oppnå miljømål, ved å tildele tilstrekkelige ressurser, herunder offentlig finansiering og unionsfinansiering, og, dersom det er hensiktsmessig og kvalifikasjons- og utvelgelseskriteriene er oppfylt, ved særlig å ta høyde for prosjekter som forfølger slike mål. Slike prosjekter bør bygge på prinsippet om tverrfaglig samarbeid mellom KI-utviklere, eksperter på ulikhet og ikke-diskriminering, tilgjengelighet, forbrukerrettigheter, miljørettigheter 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 oppstartsbedrifter, som er leverandører eller idriftsettere av KI-systemer. For dette formålet bør medlemsstatene utarbeide initiativer som er rettet mot disse operatørene, herunder når det gjelder bevisstgjøring og informasjon. Medlemsstatene bør gi små og mellomstore bedrifter, herunder oppstartsbedrifter, som har et forretningskontor eller en filial i Unionen, prioritert tilgang til de regulatoriske sandkassene for KI, forutsatt at de oppfyller kvalifikasjonsvilkårene og utvelgelseskriteriene, og uten å hindre at andre leverandører og prospektive leverandører får tilgang til sandkassene, forutsatt at de samme vilkårene og kriteriene er oppfylt. Medlemsstatene bør benytte eksisterende kanaler og, dersom det er hensiktsmessig, opprette nye særskilte kanaler for kommunikasjon med små og mellomstore bedrifter, herunder oppstartsbedrifter, samt idriftsettere, andre innovatører og, dersom det er hensiktsmessig, lokale offentlige myndigheter, for å støtte små og mellomstore bedrifter gjennom hele utviklingsforløpet ved å gi veiledning og svare på

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

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

spørsmål om gjennomføringen av denne forordningen. Når det er hensiktsmessig, bør disse kanalene samarbeide for å skape synergier og sikre ensartethet i veiledningen til små og mellomstore bedrifter, herunder oppstartsbedrifter, og idriftsettere. I tillegg bør medlemsstatene legge til rette for at små og mellomstore bedrifter og andre relevante berørte parter kan delta i prosessene for utarbeiding av standarder. Videre bør det tas hensyn til de særskilte interessene og behovene til leverandører som er små og mellomstore bedrifter, herunder oppstartsbedrifter, når meldte organer fastsetter gebyrer for samsvarsvurdering. Kommisjonen bør jevnlig vurdere sertifiserings- og etterlevelseskostnadene for små og mellomstore bedrifter, herunder oppstartsbedrifter, gjennom åpne konsultasjoner og bør samarbeide med medlemsstatene for å redusere slike kostnader. For eksempel kan oversettelseskostnader knyttet til obligatorisk dokumentasjon og kommunikasjon med myndigheter utgjøre en betydelig kostnad for leverandører og andre operatører, særlig de som er av mindre skala. Medlemsstatene bør eventuelt sikre at et av de språkene som de fastsetter og aksepterer for relevante leverandørers dokumentasjon og for kommunikasjon med operatører, er et språk som generelt forstås av flest mulig idriftsettere på tvers av landegrensene. For å ivareta de særskilte behovene til små og mellomstore bedrifter, herunder oppstartsbedrifter, bør Kommisjonen utarbeide standardiserte maler for de områdene som omfattes av denne forordningen, på anmodning fra KI-rådet. I tillegg bør Kommisjonen supplere medlemsstatenes innsats ved å tilby en felles informasjonsplattform med brukervennlig informasjon om denne forordningen for alle leverandører og idriftsettere, ved å organisere egnede informasjonskampanjer for å øke bevisstheten om de forpliktelsene som følger av denne forordningen, og ved å evaluere og fremme konvergens mellom beste praksis i prosedyrene for offentlige anskaffelser i forbindelse med KI-systemer. Mellomstore bedrifter som inntil nylig kvalifiserte som små bedrifter i henhold til vedlegget til kommisjonsrekommandasjon 2003/361/EF⁽⁴⁴⁾, bør ha tilgang til disse støttetiltakene, ettersom disse nye mellomstore bedriftene noen ganger kan mangle de juridiske ressursene og den opplæringen som er nødvendig for å sikre at denne forordningen forstås riktig og overholdes.

- 144) For å fremme og beskytte innovasjon bør plattformen for KI på bestilling (AI-on-demand, AIoD) og alle relevante EU-finansieringsprogrammer og -prosjekter som gjennomføres av Kommisjonen og medlemsstatene på unionsplan eller nasjonalt plan, alt etter hva som er relevant, bidra til å nå målene i denne forordningen, for eksempel programmet for et digitalt Europa og Horisont Europa.
- 145) For å minimere risikoen for gjennomføringen på grunn av manglende kunnskap og ekspertise på markedet, og for å gjøre det lettere for leverandører, særlig små og mellomstore bedrifter, herunder oppstartsbedrifter, og meldte organer å overholde sine forpliktelser etter denne forordningen, bør AI-on-demand-plattformen, de europeiske digitale innovasjonsnavene og test- og forsøksanleggene som er opprettet av Kommisjonen og medlemsstatene på unionsplan eller nasjonalt plan, bidra til gjennomføringen av denne forordningen. Innenfor sine respektive oppdrag og kompetanseområder kan AI-on-demand-plattformen, de europeiske digitale innovasjonsnavene og test- og forsøksanleggene særlig gi teknisk og vitenskapelig støtte til leverandører og meldte organer.
- 146) Ettersom noen operatører er av svært liten størrelse, og for å sikre at innovasjonskostnadene er forholdsmessige, bør svært små bedrifter dessuten få mulighet til å oppfylle en av de mest kostbare forpliktelsene, nemlig å innføre et kvalitetsstyringssystem, på en forenklet måte som vil redusere disse bedriftenes kostnader og administrative byrde uten at det påvirker nivået av beskyttelse og nødvendigheten av å oppfylle kravene som gjelder for KI-systemer med høy risiko. Kommisjonen bør utarbeide retningslinjer for å spesifisere hvilke elementer i kvalitetsstyringssystemet som svært små bedrifter skal oppfylle på denne forenklete måten.
- 147) Kommisjonen bør i størst mulig grad lette tilgangen til test- og forsøksanlegg for organer, grupper eller laboratorier som er etablert eller akkreditert i samsvar med relevant EU-harmoniseringsregelverk, og som utfører oppgaver i forbindelse med samsvarsvurdering av produkter eller utstyr som omfattes av dette EU-harmoniseringsregelverket. Dette gjelder særlig for ekspertpaneler, ekspertlaboratorier og referanselaboratorier på området medisinsk utstyr i henhold til forordning (EU) 2017/745 og (EU) 2017/746.
- 148) Det bør fastsettes en forvaltningsramme ved denne forordningen som både gjør det mulig å samordne og støtte anvendelsen av forordningen på nasjonalt plan, å bygge opp kapabiliteter på unionsplan og å integrere berørte parter på KI-området. En effektiv gjennomføring og håndhevelse av denne forordningen krever en forvaltningsramme som gjør det mulig å bygge opp og samordne sentral ekspertise på unionsplan. KI-kontoret ble opprettet ved en kommisjonsbeslut-

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

ning⁽⁴⁵⁾ og har som oppgave å utvikle Unionens ekspertise og kapabiliteter på KI-området og bidra til gjennomføringen av Unionens regelverk om KI. Medlemsstatene bør lette KI-kontorets oppgaver for å støtte utviklingen av Unionens ekspertise og kapabiliteter på unionsplan og å styrke det digitale indre markedes funksjon. Dessuten bør det opprettes et KI-råd sammensatt av representanter for medlemsstatene, et vitenskapspanel for å involvere forskersamfunnet, og et rådgivende forum for å bidra til gjennomføringen av denne forordningen gjennom innspill fra berørte parter, på unionsplan og nasjonalt plan. Utviklingen av Unionens ekspertise og kapabiliteter bør også omfatte bruk av eksisterende ressurser og ekspertise, særlig gjennom synergier med strukturer som er bygd opp i forbindelse med håndhevelse av annen rett på unionsplan, og synergier med relaterte initiativer på unionsplan, for eksempel fellesforetaket EuroHPC og test- og forsøksanlegg for KI innenfor rammen av programmet for et digitalt Europa.

- 149) For å lette en smidig, effektiv og harmonisert gjennomføring av denne forordningen bør det opprettes et KI-råd. KI-rådet bør gjenspeile de ulike interessene innenfor KI-økosystemet og være sammensatt av representanter for medlemsstatene. KI-rådet bør ha ansvar for en rekke rådgivende oppgaver, herunder å gi uttalelser, anbefalinger og råd samt bidra til veiledning om forhold knyttet til gjennomføringen av denne forordningen, herunder om håndhevelsesspørsmål, tekniske spesifikasjoner eller eksisterende standarder relatert til kravene som fastsettes i denne forordningen, og å gi råd til Kommisjonen og medlemsstatene og deres nasjonale vedkommende myndigheter om særlige KI-spørsmål. For å gi medlemsstatene en viss fleksibilitet når de utpeker sine representanter i KI-rådet, kan slike representanter være alle personer som tilhører offentlige enheter, og som bør ha relevant kompetanse og relevante fullmakter til å lette samordningen på nasjonalt plan og bidra til at KI-rådet utfører sine oppgaver. KI-rådet bør opprette to faste undergrupper for å skape en plattform for samarbeid og utveksling mellom markedstilsynsmyndigheter og meldermyndigheter om spørsmål knyttet til henholdsvis markedstilsyn og meldte organer. Den faste undergruppen for markedstilsyn bør fungere som den administrative samarbeidsgruppen for denne forordningen i henhold til artikkel 30 i forordning (EU) 2019/1020. I samsvar med artikkel 33 i nevnte forordning bør Kommisjonen støtte virksomheten til den faste undergruppen for markedstilsyn ved å gjennomføre markedsevalueringer eller -undersøkelser, særlig med sikte på å identifisere aspekter av denne forordningen som krever særskilt og rask samordning mellom markedstilsynsmyndigheter. KI-rådet kan opprette andre faste eller midlertidige undergrupper etter behov for å behandle særlige spørsmål. KI-rådet bør også, når det er hensiktsmessig, samarbeide med relevante unionsorganer, ekspertgrupper og nettverk som arbeider innenfor rammen av relevant unionsrett, særlig de som arbeider i henhold til relevant unionsrett om data digitale produkter og tjenester.
- 150) Med sikte på å sikre at berørte parter involveres i gjennomføringen og anvendelsen av denne forordningen, bør det opprettes et rådgivende forum som rådgir og yter teknisk ekspertise til KI-rådet og Kommisjonen. For å sikre en variert og balansert representasjon av berørte parter mellom kommersielle og ikke-kommersielle interesser og innad i kategorien kommersielle interesser, med hensyn til små og mellomstore bedrifter og andre foretak, bør det rådgivende forumet omfatte blant annet industri, oppstartsbedrifter, små og mellomstore bedrifter, academia, sivilsamfunnet, herunder partene i arbeidslivet, samt byrået for grunnleggende rettigheter, ENISA, Den europeiske standardiseringsorganisasjon (CEN), Den europeiske komité for elektroteknisk standardisering (CENELEC) og Det europeiske standardiseringsinstitutt for telekommunikasjoner (ETSI).
- 151) For å støtte gjennomføringen og håndhevelsen av denne forordningen, særlig KI-kontorets overvåkingsvirksomhet med hensyn til allmenne KI-modeller, bør det opprettes et vitenskapspanel av uavhengige eksperter. De uavhengige ekspertene som utgjør vitenskapspanelet, bør velges på grunnlag av oppdatert vitenskapelig eller teknisk ekspertise på KI-området og bør utføre sine oppgaver på en upartisk og objektiv måte og sikre fortrolig behandling av opplysninger og data som de mottar under utøvelsen av sitt arbeid. For å gjøre det mulig å styrke den nasjonale kapasiteten som er nødvendig for en effektiv håndhevelse av denne forordningen, bør medlemsstatene kunne anmode om støtte fra den gruppen av eksperter som utgjør vitenskapspanelet for deres håndhevelsesaktiviteter.
- 152) For å bidra til en tilfredsstillende håndhevelse av reglene for KI-systemer og styrke kapasiteten i medlemsstatene bør det opprettes EU-støttestrukturer for KI-testing som gjøres tilgjengelige for medlemsstatene.
- 153) Medlemsstatene har en nøkkelrolle i anvendelsen og håndhevelsen av denne forordningen. I den forbindelse bør hver medlemsstat utpeke minst én meldermyndighet og minst én markedstilsynsmyndighet som nasjonale vedkommende myndigheter med henblikk på å føre tilsyn med anvendelsen og gjennomføringen av denne forordningen. Medlemsstatene kan beslutte å utpeke enhver type offentlig enhet til å utføre de nasjonale vedkommende myndighetenes oppgaver i henhold til denne forordningen, i samsvar med sine særlige nasjonale organisatoriske kjennetegn og behov. For å gjøre organisasjonen mer effektiv for medlemsstatene og opprette et felles kontaktpunkt overfor allmennheten og andre motparter på medlemsstats- og unionsplan bør hver medlemsstat utpeke en markedstilsynsmyndighet som skal fungere som et felles kontaktpunkt.

⁽⁴⁵⁾ Kommisjonsbeslutning av 24.1.2024 om opprettelse av Det europeiske kontoret for kunstig intelligens C(2024) 390.

- 154) De nasjonale vedkommende myndighetene bør utøve sine fullmakter på en uavhengig, upartisk måte og uten forutinntatthet for å ivareta objektivitetsprinsippet i sine aktiviteter og oppgaver, og for å sørge for at denne forordningen anvendes og gjennomføres. Medlemmene av disse myndighetene bør avholde seg fra enhver handling som er uforenlig med deres verv, og bør være underlagt regler om taushetsplikt i henhold til denne forordningen.
- 155) For å sikre at leverandører av KI-systemer med høy risiko kan ta hensyn til erfaringene med bruk av KI-systemer med høy risiko for å forbedre sine systemer og sin utformings- og utviklingsprosess eller raskt kan treffe eventuelle korrigerende tiltak, bør alle leverandører ha et system for overvåking etter omsetning. Dersom det er relevant, bør overvåkingen etter omsetning omfatte en analyse av samhandlingen med andre KI-systemer, inkludert andre enheter og annen programvare. Overvåkingen etter omsetning bør ikke omfatte sensitive operasjonelle data tilhørende idriftsettere som er rettshåndhevende myndigheter. Dette systemet er også nøkkelen til å sikre at den mulige risikoen forbundet med KI-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 sammenhengen bør også leverandørene være pålagt å ha et system på plass for å rapportere til de relevante myndighetene om alvorlige hendelser som skyldes bruk av deres KI-systemer, det vil si hendelser eller funksjonsfeil som fører til dødsfall eller alvorlig helseskade, alvorlige og uopprettelige forstyrrelser i forvaltningen og driften av kritisk infrastruktur, overtredelser av forpliktelser i henhold til unionsretten som har til formål å verne grunnleggende rettigheter, eller alvorlig skade på eiendom eller miljøet.
- 156) For å sikre en hensiktsmessig og effektiv håndhevelse av kravene og forpliktelsene som fastsettes ved denne forordningen, som er en del av Unionens harmoniseringsregelverk, bør systemet med markedstilsyn og produktsamsvar som er innført ved forordning (EU) 2019/1020, gjelde i sin helhet. Markedstilsynsmyndigheter som er utpekt i samsvar med denne forordningen, bør ha alle håndhevelsesfullmakter som er fastsatt i denne forordningen og i forordning (EU) 2019/1020, og bør utøve sine fullmakter og oppfylle sine forpliktelser på en uavhengig og upartisk måte uten forutinntatthet. Selv om flertallet av KI-systemer ikke er omfattet av særlige krav og forpliktelser etter denne forordningen, kan markedstilsynsmyndighetene treffe tiltak med hensyn til alle KI-systemer når de utgjør en risiko i samsvar med denne forordningen. På grunn av den særlige karakteren til de av Unionens institusjoner, byråer og organer som faller inn under denne forordningens virkeområde, bør EUs datatilsyn utpekes som vedkommende markedstilsynsmyndighet for dem. Dette bør ikke berøre medlemsstatenes utpeking av nasjonale vedkommende myndigheter. Markedstilsynsvirkomheten bør ikke være til hinder for at enhetene som er underlagt tilsyn, kan utføre sine oppgaver på en uavhengig måte, når slik uavhengighet kreves i henhold til unionsretten.
- 157) Denne forordningen berører ikke kompetansen, oppgavene, fullmaktene og uavhengigheten til relevante nasjonale offentlige myndigheter eller organer som fører tilsyn med anvendelsen av unionsretten om vern av grunnleggende rettigheter, herunder likestillingsorganer og personvernmyndigheter. Når 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 forordningen. Det bør fastsettes en særskilt prosedyre for å sikre at det raskt blir truffet egnede tiltak mot KI-systemer som utgjør en risiko for helse, sikkerhet og grunnleggende rettigheter. Prosedyren bør anvendes på KI-systemer med høy risiko som utgjør en slik risiko, forbudte systemer som er brakt i omsetning, tatt i bruk eller brukt til praksis som er forbudt etter denne forordningen, og KI-systemer som er gjort tilgjengelige i strid med åpenhetskravene fastsatt i denne forordningen og utgjør en risiko.
- 158) Unionsretten om finansielle tjenester omfatter regler og krav med hensyn til interne styreformer og risikostyring som gjelder for regulerte finansinstitusjoner i forbindelse med levering av disse tjenestene, herunder når de gjør bruk av KI-systemer. For å sikre ensartet anvendelse og håndhevelse av forpliktelsene i denne forordningen og relevante regler og krav i Unionens rettsakter om finansielle tjenester bør vedkommende myndigheter for tilsyn med og håndhevelse av disse rettsaktene, særlig vedkommende myndigheter som definert i europaparlaments- og rådsforordning (EU) nr. 575/2013⁽⁴⁶⁾ og europaparlaments- og rådsdirektiv 2008/48/EF⁽⁴⁷⁾, 2009/138/EF⁽⁴⁸⁾, 2013/36/EU⁽⁴⁹⁾,

⁽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 forbrukerkredittavtaler og om oppheving 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 å starte og utøve virksomhet innen forsikring og gjenforsikring (Solvens II) (EUT L 335 av 17.12.2009, s. 1).

⁽⁴⁹⁾ Europaparlaments- og rådsdirektiv 2013/36/EU av 26. juni 2013 om adgang til å utøve virksomhet som kredittinstitusjon 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).

2014/17/EU⁽⁵⁰⁾ og (EU) 2016/97⁽⁵¹⁾, utpekes innenfor sine respektive kompetanseområder som vedkommende myndigheter for å føre tilsyn med gjennomføringen av denne forordningen, også markedstilsynsvirksomhet, med hensyn til KI-systemer som leveres eller brukes av regulerte finansinstitusjoner og finansinstitusjoner under tilsyn, med mindre medlemsstatene beslutter å utpeke en annen myndighet til å utføre disse markedstilsynsoppgavene. Disse vedkommende myndighetene bør ha alle fullmakter i henhold til denne forordningen og forordning (EU) 2019/1020 til å håndheve kravene og forpliktelsene i denne forordningen, herunder fullmakter til å gjennomføre markedstilsynsvirksomhet i ettertid som, alt etter hva som er relevant, kan integreres i deres eksisterende tilsynsordninger og -prosedyrer i henhold til den relevante unionsretten om finansielle tjenester. Når de fungerer som markedstilsynsmyndigheter i henhold til denne forordningen, bør de nasjonale tilsynsmyndighetene med ansvar for tilsynet med kredittinstitusjoner som er regulert i henhold til direktiv 2013/36/EU, og som deltar i den felles tilsynsordningen opprettet ved rådsforordning (EU) nr. 1024/2013⁽⁵²⁾, uten ugrunnet opphold rapportere til Den europeiske sentralbank alle opplysninger identifisert i forbindelse med deres markedstilsynsaktiviteter som kan være av interesse for Den europeiske sentralbanks tilsynsoppgaver som angitt i nevnte forordning. For ytterligere å bedre konsekvensen mellom denne forordningen og de reglene som gjelder for kredittinstitusjoner som er regulert av direktiv 2013/36/EU, bør også noen av leverandørenes prosedyremessige forpliktelser når det gjelder risikostyring, overvåking etter omsetning og dokumentasjon, integreres i de eksisterende forpliktelsene og prosedyrene i henhold til direktiv 2013/36/EU. For å unngå overlapping bør det også fastsettes begrensede unntak med hensyn til leverandørers kvalitetsstyringssystem og den tilsynsplikten som pålegges idriftsettere av KI-systemer med høy risiko, i den utstrekningen disse bestemmelsene gjelder for kredittinstitusjoner 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 med hensyn til interne styreformer, ordninger eller prosesser som er fastsatt i samsvar med den relevante unionsretten om finansielle tjenester, for å sikre konsekvens og likebehandling i finanssektoren.

- 159) Hver markedstilsynsmyndighet for KI-systemer med høy risiko på området biometri, som oppført i et vedlegg til denne forordningen, bør i den grad disse systemene brukes med henblikk på rettshåndhevelse, migrasjons-, asyl- og grensekontrollforvaltning eller rettspleie og demokratiske prosesser, ha effektive etterforskningsfullmakter og korrigerende fullmakter, herunder minst fullmakt til å skaffe seg tilgang til alle personopplysninger som behandles, og til alle opplysninger som er nødvendige for at markedstilsynsmyndigheten skal kunne utføre sine oppgaver. Markedstilsynsmyndighetene bør kunne utøve sine fullmakter i full uavhengighet. Enhver begrensning av deres tilgang til sensitive operasjonelle data i henhold til denne forordningen, bør ikke berøre de fullmaktene de er gitt ved direktiv (EU) 2016/680. Ingen bestemmelse i denne forordningen som utelukker utlevering av data til nasjonale personvernmyndigheter, bør berøre disse myndighetenes nåværende eller framtidige fullmakter utenfor denne forordningens virkeområde.
- 160) Markedstilsynsmyndighetene og Kommisjonen bør kunne foreslå felles aktiviteter, herunder felles undersøkelser, som skal utføres av markedstilsynsmyndighetene eller av markedstilsynsmyndighetene i fellesskap med Kommisjonen, og som har som mål å fremme samsvar, påvise manglende samsvar, øke bevisstheten om og gi veiledning om denne forordningen med hensyn til bestemte kategorier av KI-systemer med høy risiko som viser seg å utgjøre en alvorlig risiko i to eller flere medlemsstater. Felles aktiviteter for å fremme samsvar bør utføres i samsvar med artikkel 9 i forordning (EU) 2019/1020. KI-kontoret bør sørge for samordningsstøtte ved felles undersøkelser.
- 161) Det er nødvendig å klargjøre ansvars- og kompetanseområdene på unionsplan og nasjonalt plan når det gjelder KI-systemer som bygger på KI-modeller for allmenne formål. For å unngå kompetanseoverlapping når et KI-system er basert på KI-modell for allmenne formål, og modellen og systemet er levert av samme leverandør, bør tilsynet skje på unionsplan gjennom KI-kontoret, som for dette formålet bør ha fullmaktene til en markedstilsynsmyndighet som definert i forordning (EU) 2019/1020. I alle andre tilfeller er de nasjonale markedstilsynsmyndighetene ansvarlige for tilsynet med KI-systemer. For KI-systemer for allmenne formål som kan brukes direkte av idriftsettere for minst ett formål som er klassifisert som et formål med høy risiko, bør imidlertid markedstilsynsmyndighetene samarbeide med KI-kontoret om å gjennomføre evalueringer av samsvar og underrette KI-rådet og andre markedstilsynsmyndigheter om

⁽⁵⁰⁾ Europaparlaments- og rådsdirektiv 2014/17/EU av 4. februar 2014 om kredittavtaler for forbrukere i forbindelse med fast eiendom til boligformål 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 tildeling av særskilte oppgaver til Den europeiske sentralbank i forbindelse med politikken for tilsyn med kredittinstitusjoner (EUT L 287 av 29.10.2013, s. 63).

dette. Dessuten bør markedstilsynsmyndighetene kunne be om bistand fra KI-kontoret dersom markedstilsynsmyndigheten ikke er i stand til å fullføre en undersøkelse av et KI-system med høy risiko fordi den ikke får tilgang til visse opplysninger om den KI-modellen for allmenne formål som KI-systemet med høy risiko bygger på. I slike tilfeller bør prosedyren for gjensidig bistand over landegrensene i kapittel VI i forordning (EU) 2019/1020 gjelde tilsvarende med nødvendige endringer.

- 162) For å utnytte Unionens sentraliserte ekspertise og synergier på best mulig måte på unionsplan bør myndigheten til å føre tilsyn med og håndheve forpliktelsene for leverandører av KI-modeller for allmenne formål ligge hos Kommisjonen. KI-kontoret bør kunne iverksette alle nødvendige tiltak for å kontrollere at denne forordningen gjennomføres effektivt med hensyn til KI-modeller for allmenne formål. Den bør kunne undersøke mulige overtredelser av reglene for leverandører av KI-modeller for allmenne formål både på eget initiativ og på anmodning fra markedstilsynsmyndighetene i samsvar med vilkårene i denne forordningen. For å bidra til at KI-kontorets overvåking er effektiv, bør KI-kontoret gi nedstrømsleverandører mulighet til å klage på mulige overtredelser av reglene for leverandører av KI-modeller og -systemer for allmenne formål.
- 163) Med sikte på å supplere forvaltningssystemene for KI-modeller for allmenne formål bør vitenskapspanelet støtte KI-kontorets overvåkingsvirksomhet og kan i visse tilfeller gi KI-kontoret kvalifiserte varsler som utløser oppfølging, for eksempel undersøkelser. Dette bør være tilfellet dersom vitenskapspanelet har grunn til å mistenke at en KI-modell for allmenne formål utgjør en konkret og identifiserbar risiko på unionsplan. Det bør også være tilfellet dersom vitenskapspanelet har grunn til å mistenke at en KI-modell for allmenne formål oppfyller kriteriene for å bli klassifisert som en KI-modell for allmenne formål med systemrisiko. For at vitenskapspanelet skal få den informasjonen som er nødvendig for å utføre disse oppgavene, bør det finnes en ordning der vitenskapspanelet kan anmode Kommisjonen om å kreve dokumentasjon eller informasjon fra en leverandør.
- 164) KI-kontoret bør kunne treffe nødvendige tiltak for å kontrollere at de forpliktelsene for leverandører av KI-modeller for allmenne formål som er fastsatt i denne forordningen, effektivt gjennomføres og overholdes. KI-kontoret bør kunne etterforske mulige overtredelser i samsvar med fullmaktene fastsatt i denne forordningen, blant annet ved å be om dokumentasjon og informasjon, foreta evalueringer og be om tiltak fra leverandører av KI-modeller for allmenne formål. For å benytte seg av uavhengig ekspertise ved gjennomføring av evalueringer bør KI-kontoret kunne bruke uavhengige eksperter til å utføre evalueringene på sine vegne. Oppfyllelse av forpliktelsene bør kunne håndheves blant annet ved anmodning om å treffe egnede tiltak, herunder risikoreducerende tiltak ved påvist systemrisiko, og ved at tilgjengeliggjøring av modellen på markedet begrenses, eller at modellen trekkes tilbake eller tilbakekalles. Som et sikkerhetstiltak bør leverandører av KI-modeller for allmenne formål, dersom det er nødvendig utover de prosessuelle rettighetene fastsatt i denne forordningen, ha de prosessuelle rettighetene fastsatt i artikkel 18 i forordning (EU) 2019/1020, som bør gjelde tilsvarende med nødvendige endringer, uten at det berører mer spesifikke prosessuelle rettigheter fastsatt i denne forordningen.
- 165) Utvikling av andre KI-systemer enn KI-systemer med høy risiko i samsvar med kravene i denne forordningen kan føre til større utbredelse av etisk og pålitelig KI i Unionen. Leverandører av KI-systemer som ikke er KI-systemer med høy risiko, bør oppmuntres til å utarbeide atferdsregler, herunder tilhørende forvaltningsmekanismer, som har til hensikt å fremme frivillig anvendelse av noen av eller alle de obligatoriske kravene som gjelder for KI-systemer med høy risiko, tilpasset i lys av det tiltenkte formålet med systemene og den lavere risikoen som er involvert, og idet det tas hensyn til tilgjengelige tekniske løsninger og bransjens beste praksis, for eksempel modell- og datakort. Leverandører og eventuelt idriftsettere av alle KI-systemer, med eller uten høy risiko, og KI-modeller bør også oppfordres til på frivillig basis å anvende ytterligere krav knyttet til for eksempel deler av Unionens etiske retningslinjer for pålitelig KI, miljømessig bærekraft, tiltak for KI-kompetanse, inkluderende og mangfoldig utforming og utvikling av KI-systemer, herunder hensyn til sårbare personer og tilgjengelighet for personer med nedsatt funksjonsevne, berørte parter deltakelse, eventuelt med medvirkning fra relevante berørte parter, som næringslivs- og sivilsamfunnsorganisasjoner, akademier, forskningsorganisasjoner, fagforeninger og forbrukerorganisasjoner, i utformingen og utviklingen av KI-systemer, samt mangfold i utviklingsteamene, herunder kjønnsbalanse. For å sikre at de frivillige atferdsreglene er effektive, bør de være basert på klare mål og nøkkeltallsindikatorer for å måle oppnåelsen av disse målene. De bør også utvikles på en inkluderende må-

te og, dersom det er relevant, med medvirkning fra relevante berørte parter, som næringslivs- og sivilsamfunnsorganisasjoner, academia, forskningsorganisasjoner, fagforeninger og forbrukerorganisasjoner. Kommisjonen kan utvikle initiativer, også av sektorspesifikk art, for å redusere tekniske hindre mot grensekryssende utveksling av data til KI-utvikling, herunder når det gjelder datatilgangsinfrastruktur og semantisk og teknisk interoperabilitet mellom ulike typer data.

- 166) Det er viktig at KI-systemer som er knyttet til produkter som ikke har høy risiko etter denne forordningen, og som dermed ikke må oppfylle kravene som gjelder for KI-systemer med høy risiko, likevel er sikre når de bringes i omsetning eller tas i bruk. For å bidra til dette målet vil europaparlaments- og rådsforordning (EU) 2023/988⁽⁵³⁾ få anvendelse som et sikkerhetsnett.
- 167) For å sikre et tillitsfullt og konstruktivt samarbeid mellom vedkommende myndigheter på unionsplan og nasjonalt plan, bør alle parter som deltar i anvendelsen av denne forordningen, i samsvar med unionsretten eller nasjonal rett respektere fortroligheten av opplysninger og data som de mottar når de utfører sine oppgaver. De bør utføre sine oppgaver og aktiviteter på en måte som særlig beskytter immaterielle rettigheter, fortrolig forretningsinformasjon og forretningshemmeligheter, effektiv gjennomføring av denne forordningen, offentlige og nasjonale sikkerhetsinteresser, integriteten til straffesaker og forvaltningssaker og integriteten til graderte opplysninger.
- 168) Denne forordningen bør kunne håndheves ved å ilegge sanksjoner og andre håndhevelsestiltak. Medlemsstatene bør treffe alle nødvendige tiltak for å sikre at bestemmelsene i denne forordningen gjennomføres, herunder ved å fastsette effektive, forholdsmessige og avskrekkende sanksjoner ved brudd på bestemmelsene, og ved å overholde prinsippet om at samme overtredelse ikke skal straffes to ganger. For å styrke og harmonisere de administrative sanksjonene for overtredelse av denne forordningen bør det fastsettes øvre grenser for gebyrene som kan ilegges ved visse spesifikke overtredelser. Når medlemsstatene vurderer overtredelsesgebyrenes størrelse, bør de i hvert enkelt tilfelle ta alle relevante forhold i den bestemte situasjonen i betraktning og ta behørig hensyn særlig til overtredelsens art, grovhet, varighet og konsekvenser samt til leverandørens størrelse, særlig dersom leverandøren er en liten eller mellomstor bedrift, herunder en oppstartsbedrift. EUs datatilsyn bør ha myndighet til å ilegge overtredelsesgebyrer til de av Unionens institusjoner, byråer og organer som faller inn under denne forordningens virkeområde.
- 169) De forpliktelsene som pålegges leverandører av KI-modeller for allmenne formål i henhold til denne forordningen, bør kunne håndheves blant annet ved å ilegge overtredelsesgebyrer. For dette formålet bør det også fastsettes passende nivåer på gebyrene for overtredelse av disse forpliktelsene, herunder for tilsidesettelse av tiltak som Kommisjonen krever i samsvar med denne forordningen, med forbehold for passende foreldelsesfrister i samsvar med forholdsmessighetsprinsippet. Alle beslutninger som Kommisjonen treffer i henhold til denne forordningen, kan prøves av Den europeiske unions domstol i samsvar med TEUV, herunder Domstolens fullstendige domsmyndighet med hensyn til sanksjoner i samsvar med artikkel 261 i TEUV.
- 170) EU-retten og nasjonal rett gir allerede effektive rettsmidler til fysiske og juridiske personer hvis rettigheter og friheter påvirkes negativt av bruken av KI-systemer. Uten at det berører disse rettsmidlene, bør enhver fysisk eller juridisk person som har grunn til å anta at det foreligger en overtredelse av denne forordningen, ha rett til å klage til den relevante markedstilsynsmyndigheten.
- 171) Berørte personer bør ha rett til å få en forklaring dersom en idriftsetters beslutning i hovedsak er basert på utdata fra visse KI-systemer med høy risiko som faller inn under denne forordningens virkeområde, og dersom denne beslutningen har rettsvirkninger eller på lignende måte i betydelig grad påvirker disse personene på en måte som de anser for å ha en negativ innvirkning på deres helse, sikkerhet eller grunnleggende rettigheter. Denne forklaringen bør være klar og meningsfull, og den bør utgjøre et grunnlag for de berørte personenes utøvelse av sine rettigheter. Retten til å få en forklaring bør ikke gjelde for bruk av KI-systemer som omfattes av unntak eller restriksjoner etter unionsretten eller nasjonal rett, og bør bare gjelde i den grad denne rettigheten ikke allerede er fastsatt i unionsretten.

⁽⁵³⁾ Europaparlaments- og rådsforordning (EU) 2023/988 av 10. mai 2023 om alminnelig 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).

- 172) Personer som opptrer som varslere i forbindelse med overtredelser av denne forordningen, bør beskyttes i henhold til unionsretten. Europaparlaments- og rådsdirektiv (EU) 2019/1937⁽⁵⁴⁾ bør derfor få anvendelse på rapportering av overtredelser av denne forordningen og på beskyttelse for personer som rapporterer slike overtredelser.
- 173) For å sikre at regelverket kan tilpasses når 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 som et KI-system med høy risiko, listen over KI-systemer med høy risiko, bestemmelsene om teknisk dokumentasjon, innholdet i EU-samsvarserklæringen, bestemmelsene om samsvarsvurderingsprosedyren, bestemmelsene om fastsettelse av hvilke KI-systemer med høy risiko som samsvarsvurderingsprosedyren basert på vurdering av kvalitetsstyringssystemet og vurdering av den tekniske dokumentasjonen bør anvendes på, terskelen, referansene og indikatorene, herunder ved å supplere disse referansene og indikatorene, i reglene for klassifisering av KI-modeller for allmenne formål med systemrisiko, kriteriene for utpeking av KI-modeller for allmenne formål med systemrisiko, den tekniske dokumentasjonen for leverandører av KI-modeller for allmenne formål og åpenhetsinformasjonen for leverandører av KI-modeller for allmenne formål. Det er særlig viktig at Kommisjonen holder hensiktsmessige samråd under sitt forberedende arbeid, herunder på ekspertnivå, og at slike samråd gjennomføres i samsvar med prinsippene fastsatt i den tverrinstitusjonelle avtalen av 13. april 2016 om bedre regelverksutforming⁽⁵⁵⁾. For å sikre lik deltakelse i forberedelsen av delegerede rettsakter er det også viktig at Europaparlamentet og Rådet mottar alle dokumenter samtidig som medlemsstatenes sakkyndige, og at deres eksperter gis systematisk adgang til møter i Kommisjonens ekspertgrupper som omhandler forberedelsen av delegerede rettsakter.
- 174) I betraktning av den raske teknologiske utviklingen og den tekniske ekspertisen som kreves for å anvende denne forordningen effektivt, bør Kommisjonen evaluere og revidere denne forordningen innen 2. august 2029 og deretter hvert fjerde år, og avlegge rapport til Europaparlamentet og Rådet. I tillegg bør Kommisjonen, idet den tar hensyn til konsekvensene for denne forordningens virkeområde, en gang i året foreta en vurdering av behovet for å endre listen over KI-systemer med høy risiko og listen over forbudt praksis. Innen 2. august 2028 og deretter hvert fjerde år bør Kommisjonen dessuten vurdere og rapportere til Europaparlamentet og Rådet om behovet for å endre listen over rubrikker for bruksområder med høy risiko i vedlegget til denne forordningen, de KI-systemene som omfattes av åpenhetsforpliktelsene, effektiviteten av tilsyns- og forvaltningssystemet og framskrittene i utvikling av standardiseringspublikasjoner om energieffektiv utvikling av KI-modeller for allmenne formål, herunder behovet for ytterligere forholdsregler og tiltak. Endelig bør Kommisjonen innen 2. august 2028 og deretter hvert tredje år evaluere innvirkningen og effektiviteten av frivillige atferdsregler for å fremme anvendelse av de kravene som er fastsatt for KI-systemer med høy risiko, på andre KI-systemer enn KI-systemer med høy risiko, og eventuelt av andre ytterligere krav til slike KI-systemer.
- 175) For å sikre ensartede vilkår for gjennomføringen av denne forordningen bør Kommisjonen gis gjennomføringsmyndighet. Denne myndigheten bør utøves i samsvar med europaparlaments- og rådsforordning (EU) nr. 182/2011⁽⁵⁶⁾.
- 176) Ettersom målet for denne forordningen, som er å forbedre det indre markedes virkemåte og fremme utbredelsen av menneskesentrert og pålitelig KI, samtidig som det sikres et høyt vernivå for helse, sikkerhet og grunnleggende rettigheter som er nedfelt i pakten, herunder demokrati, rettsstatsprinsippet og miljøvern, mot skadelige virkninger av KI-systemer i Unionen, og å støtte innovasjon, ikke kan nås i tilstrekkelig grad av medlemsstatene og derfor på grunn av tiltakets omfang eller virkninger bedre kan nås på unionsplan, kan Unionen treffe tiltak i samsvar med nærhetsprinsippet som fastsatt i artikkel 5 i TEU. I samsvar med forholdsmessighetsprinsippet fastsatt i nevnte artikkel går denne forordningen ikke lenger enn det som er nødvendig for å nå dette målet.
- 177) For å sikre rettslig forutsigbarhet, sikre en hensiktsmessig tilpasningsperiode for operatører og unngå markedsforstyrrelser, herunder ved å sikre kontinuitet i bruken av KI-systemer, bør denne forordningen få anvendelse på KI-systemer med høy risiko som er brakt i omsetning eller tatt i bruk før forordningens generelle anvendelsesdato, bare dersom disse systemene fra og med den datoen er gjenstand for betydelige endringer i sin utforming eller sitt tiltenkte formål. Det bør

⁽⁵⁴⁾ Europaparlaments- og rådsdirektiv (EU) 2019/1937 av 23. oktober 2019 om beskyttelse for personer som rapporterer overtredelser av 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 allmenne regler og prinsipper for medlemsstatenes kontroll med Kommisjonens utøvelse av sin gjennomføringsmyndighet (EUT L 55 av 28.2.2011, s. 13).

presiseres at begrepet «betydelig endring» i denne forbindelsen bør forstås som innholdsmessig likeverdig med begrepet «vesentlig endring», som bare brukes om KI-systemer med høy risiko i henhold til denne forordningen. I unntakstilfeller og i lys av offentlig ansvarlighet bør operatører av KI-systemer som er komponenter i de store IT-systemene som er opprettet ved de rettsaktene som er oppført i et vedlegg til denne forordningen, og operatører av KI-systemer med høy risiko som skal brukes av offentlige myndigheter, treffe de nødvendige tiltakene for å oppfylle kravene i denne forordningen henholdsvis innen utgangen av 2030 og innen 2. august 2030.

- 178) Leverandører av KI-systemer med høy risiko oppfordres til på frivillig grunnlag å begynne å oppfylle de relevante forpliktelsene i denne forordningen allerede i overgangsperioden.
- 179) Denne forordningen bør få anvendelse fra 2. august 2026. Tatt i betraktning den uakseptable risikoen som er forbundet med bruk av KI på visse måter, bør imidlertid forbudene og de allmenne bestemmelsene i denne forordningen få anvendelse allerede fra 2. februar 2025. Selv om den fulle virkningen av disse forbudene vil vise seg først når forvaltningen og håndhevelsen av denne forordningen er fastsatt, er det viktig å foregripe anvendelsen av forbudene for å ta hensyn til uakseptable risikoer og for å påvirke andre prosedyrer, for eksempel i sivilretten. Dessuten bør infrastrukturen knyttet til forvaltnings- og samsvarsvurderingssystemet være i drift før 2. august 2026, og derfor bør bestemmelsene om meldte organer og forvaltningsstruktur få anvendelse fra 2. august 2025. På grunn av det høye tempoet i den teknologiske utviklingen og i innføringen av KI-modeller for allmenne formål, bør forpliktelsene for leverandører av KI-modeller for allmenne formål få anvendelse fra 2. august 2025. Reglene for god praksis bør være klare innen 2. mai 2025, slik at leverandørene kan dokumentere overholdelse i tide. KI-kontoret bør sikre at reglene og prosedyrene for klassifisering er ajourført i lys av den teknologiske utviklingen. I tillegg bør medlemsstatene fastsette og underrette Kommisjonen om reglene for sanksjoner, herunder overtredelsesgebyrer, og sikre at de er korrekt og effektivt gjennomført innen anvendelsesdatoen for denne forordningen. Bestemmelsene om sanksjoner bør derfor få anvendelse fra 2. august 2025.
- 180) EUs datatilsyn og EUs personvernråd har blitt rådspurt i samsvar med artikkel 42 nr. 1 og 2 i forordning (EU) 2018/1725 og avga sin felles uttalelse 18. juni 2021.

VEDTATT DENNE FORORDNINGEN:

KAPITTEL I

ALMINNELIGE BESTEMMELSER

Artikkel 1

Formål

1. Formålet med denne forordningen er å forbedre det indre markeds virkemåte og fremme utbredelse av menneskesentrert og pålitelig kunstig intelligens (KI), samtidig som det sikres et høyt vernnivå for helse, sikkerhet og grunnleggende rettigheter nedfelt i paktens, herunder demokrati, rettsstatsprinsippet og miljøvern, mot de skadelige virkningene av KI-systemer i Unionen, og å støtte innovasjon.
2. Denne forordningen fastsetter
 - a) harmoniserte regler for å bringe i omsetning, ta i bruk og bruke KI-systemer i Unionen,

- b) forbud mot visse former for KI-praksis,
- c) særlige krav til KI-systemer med høy risiko og forpliktelser for operatører av slike systemer,
- d) harmoniserte åpenhetsregler for visse KI-systemer,
- e) harmoniserte regler for å bringe i omsetning KI-modeller for allmenne formål,
- f) regler for markedsovervåking, markedstilsyn, forvaltning og håndhevelse,
- g) tiltak for å støtte innovasjon, med særlig fokus på små og mellomstore bedrifter, herunder oppstartsbedrifter.

Artikkel 2

Virkeområde

1. Denne forordningen får anvendelse på
 - a) leverandører som bringer i omsetning eller tar i bruk KI-systemer eller bringer KI-modeller for allmenne formål i omsetning i Unionen, uansett om disse leverandørene er etablert eller lokalisert i Unionen eller i et tredjeland,
 - b) idriftsettere av KI-systemer som har sitt etableringssted i eller er lokalisert i Unionen,
 - c) leverandører og idriftsettere av KI-systemer som har sitt etableringssted i eller er lokalisert i et tredjeland, dersom utdataene som produseres av KI-systemet, brukes i Unionen,
 - d) importører og distributører av KI-systemer,
 - e) produkttilvirkere som bringer i omsetning eller tar i bruk et KI-system sammen med sitt produkt og under sitt eget navn eller varemerke,
 - f) bemyndigede representanter for leverandører som ikke er etablert i Unionen,
 - g) berørte personer som er lokalisert i Unionen.

2. For KI-systemer som er klassifisert som KI-systemer med høy risiko i samsvar med artikkel 6 nr. 1 og er knyttet til produkter som omfattes av EU-harmoniseringsregelverket oppført i avsnitt B i vedlegg I, får bare artikkel 6 nr. 1, artikkel 102–109 og artikkel 112 anvendelse. Artikkel 57 får anvendelse bare i den utstrekning de kravene til KI-systemer med høy risiko som er fastsatt i denne forordningen, er blitt integrert i nevnte EU-harmoniseringsregelverk.

3. Denne forordningen får ikke anvendelse på områder utenfor unionsrettens virkeområde og skal under ingen omstendigheter berøre medlemsstatenes kompetanse med hensyn til nasjonal sikkerhet, uansett hvilken type enhet medlemsstatene har gitt i oppdrag å utføre oppgaver i forbindelse med denne kompetansen.

Denne forordningen får ikke anvendelse på KI-systemer dersom og i den grad de bringes i omsetning, tas i bruk eller brukes med eller uten tilpasning, utelukkende for militære formål, forsvarsformål eller formål knyttet til nasjonal sikkerhet, uansett hvilken type enhet som utfører disse aktivitetene.

Denne forordningen får ikke anvendelse på KI-systemer som ikke bringes i omsetning eller tas i bruk i Unionen, dersom utdataene brukes i Unionen utelukkende for militære formål, forsvarsformål eller formål knyttet til nasjonal sikkerhet, uansett hvilken type enhet som utfører disse aktivitetene.

4. Denne forordningen får verken anvendelse på offentlige myndigheter i et tredjeland eller på internasjonale organisasjoner som faller inn under virkeområdet for denne forordningen i henhold til nr. 1, dersom nevnte myndigheter eller organisasjoner bruker KI-systemer innenfor rammen av internasjonalt samarbeid eller avtaler om rettshåndhevelse og rettslig samarbeid med Unionen eller med en eller flere medlemsstater, forutsatt at et slikt tredjeland eller en slik internasjonal organisasjon gir tilstrekkelige garantier for vern av fysiske personers grunnleggende rettigheter og friheter.

5. Denne forordningen berører ikke anvendelsen av bestemmelsene om ansvar for tilbydere av formidlingstjenester som fastsatt i kapittel II i forordning (EU) 2022/2065.

6. Denne forordningen får ikke anvendelse på KI-systemer eller KI-modeller, herunder utdata fra dem, som er spesialutviklet og tatt i bruk utelukkende med henblikk på vitenskapelig forskning og utvikling.
7. Unionsretten om vern av personopplysninger, personvern og kommunikasjonsfortrolighet får anvendelse på personopplysninger som behandles i forbindelse med de rettighetene og forpliktelsene som er fastsatt i denne forordningen. Denne forordningen påvirker ikke forordning (EU) 2016/679 eller (EU) 2018/1725 eller direktiv 2002/58/EF eller (EU) 2016/680, uten at det berører artikkel 10 nr. 5 og artikkel 59 i denne forordningen.
8. Denne forordningen får ikke anvendelse på forsknings-, test- eller utviklingsaktiviteter med hensyn til 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 virkelige forhold omfattes ikke av dette unntaket.
9. Denne forordningen berører ikke reglene fastsatt i andre unionsrettsakter om forbrukervern og produktsikkerhet.
10. Denne forordningen får ikke anvendelse på de forpliktelsene som påhviler idriftsettere som er fysiske personer, og som bruker KI-systemer som ledd i rent personlige, ikke-yrkesmessige aktiviteter.
11. Denne forordningen er ikke til hinder for at Unionen eller medlemsstatene opprettholder eller innfører lover eller forskrifter som er mer fordelaktige for arbeidstakerne når det gjelder å beskytte deres rettigheter i forbindelse med arbeidsgivernes bruk av KI-systemer, eller oppmuntrer til eller tillater anvendelse av tariffavtaler som er mer fordelaktige for arbeidstakerne.
12. Denne forordningen får ikke anvendelse på KI-systemer som utgis under fri lisens med åpen kildekode, med mindre de bringes i omsetning eller tas i bruk som KI-systemer med høy risiko eller som et KI-system som omfattes av artikkel 5 eller 50.

Artikkel 3

Definisjoner

I denne forordningen menes med

- 1) «KI-system» et maskinbasert system som er konstruert for å operere med varierende grad av autonomi, som kan vise tilpasningsdyktighet etter idriftsetting, og som, for eksplisitte eller implisitte mål, ut fra inndataene det mottar, utleder hvordan man genererer utdata som prediksjoner, innhold og anbefalinger, eller beslutninger som kan påvirke fysiske eller virtuelle miljøer,
- 2) «risiko» kombinasjonen av sannsynligheten for at skade oppstår, og den aktuelle skadens alvorlighetsgrad,
- 3) «leverandør» en fysisk eller juridisk person, en offentlig myndighet, et byrå eller ethvert annet organ som utvikler et KI-system eller en KI-modell for allmenne formål, eller som får utviklet et KI-system eller en KI-modell for allmenne formål og bringer det eller den i omsetning eller tar KI-systemet i bruk under eget navn eller varemerke, mot betaling eller vederlagsfritt,
- 4) «idriftsetter» en fysisk eller juridisk person, en offentlig myndighet, et byrå eller ethvert annet organ som bruker et KI-system som er underlagt deres myndighet, unntatt når KI-systemet brukes i personlig, ikke-yrkesmessig virksomhet,
- 5) «bemyndiget representant» en fysisk eller juridisk person lokalisert eller etablert i Unionen som har fått og akseptert en skriftlig fullmakt fra en leverandør av et KI-system eller en KI-modell for allmenne formål, for henholdsvis å oppfylle og gjennomføre forpliktelsene og prosedyrene fastsatt i denne forordningen på dennes vegne,
- 6) «importør» en fysisk eller juridisk person lokalisert eller etablert i Unionen som bringer i omsetning et KI-system som bærer navnet eller varemerket til en fysisk eller juridisk person som er etablert i et tredjeland,
- 7) «distributør» enhver fysisk eller juridisk person i forsyningskjeden, utenom leverandøren eller importøren, som gjør et KI-system tilgjengelig på unionsmarkedet,
- 8) «operatør» en leverandør, produkttilvirker, idriftsetter, bemyndiget representant, importør eller distributør,

- 9) «bringe i omsetning» gjøre et KI-system eller en KI-modell for allmenne formål tilgjengelig på unionsmarkedet for første gang,
- 10) «gjøre tilgjengelig på markedet» levere et KI-system eller en KI-modell for allmenne formål for distribusjon eller bruk på unionsmarkedet i forbindelse med kommersiell virksomhet, enten mot betaling eller vederlagsfritt,
- 11) «ta i bruk» levere et KI-system til første gangs bruk direkte til idriftsetteren eller til egen bruk i Unionen for dets tiltenkte formål,
- 12) «tiltenkt formål» den bruken et KI-system er beregnet på fra leverandørens side, herunder den spesifikke sammenhengen og de spesifikke vilkårene for bruk, som angitt i informasjonen gitt av leverandøren i bruksanvisningen, markedsførings- eller salgsmateriell og uttalelser samt i den tekniske dokumentasjonen,
- 13) «rimelig forutsigbar feilbruk» bruk av et KI-system på en måte som ikke er i samsvar med det tiltenkte formålet, men som kan følge av rimelig forutsigbar menneskelig atferd eller samhandling med andre systemer, inkludert andre KI-systemer,
- 14) «sikkerhetskomponent» en komponent i et produkt eller i et KI-system som oppfyller en sikkerhetsfunksjon for det produktet eller KI-systemet, eller som ved svikt eller funksjonsfeil medfører fare for menneskers helse og sikkerhet eller for eiendom,
- 15) «bruksanvisning» informasjon fra leverandøren for å informere idriftsetteren om særlig det tiltenkte formålet med og riktig bruk av et KI-system,
- 16) «tilbakekalling av et KI-system» alle tiltak som har som formål å oppnå at et KI-system som er gjort tilgjengelig for idriftsettere, returneres til leverandøren, tas ut av drift eller deaktiveres,
- 17) «tilbaketrekking av et KI-system» alle tiltak som har som formål å hindre at et KI-system i forsyningskjeden blir gjort tilgjengelig på markedet,
- 18) «et KI-systems ytelse» et KI-systems evne til å oppnå sitt tiltenkte formål,
- 19) «meldermyndighet» den nasjonale myndigheten som er ansvarlig for å etablere og gjennomføre de nødvendige prosedyrene for vurdering, utpeking og melding av samsvarsvurderingsorganer og for tilsynet med dem,
- 20) «samsvarsvurdering» en prosess for å påvise om de kravene til et KI-system med høy risiko som er fastsatt i kapittel III avsnitt 2, er oppfylt,
- 21) «samsvarsvurderingsorgan» et organ som, som tredjepart, utfører samsvarsvurderingsaktiviteter, herunder testing, sertifisering og inspeksjon,
- 22) «meldt organ» et samsvarsvurderingsorgan som er meldt i samsvar med denne forordningen og annet relevant EU-harmoniseringsregelverk,
- 23) «vesentlig endring» en endring i et KI-system etter at det er brakt i omsetning eller tatt i bruk, som ikke er forutsett eller planlagt i den første samsvarsvurderingen utført av leverandøren, og som fører til at KI-systemets samsvar med kravene i kapittel III avsnitt 2 påvirkes, eller fører til en endring i det tiltenkte formålet som KI-systemet er vurdert for,
- 24) «CE-merking» merking der en leverandør angir at et KI-system er i samsvar med kravene i kapittel III avsnitt 2 i denne forordningen og med annet gjeldende EU-harmoniseringsregelverk for slik merking,
- 25) «system for overvåking etter omsetning», alle aktiviteter som leverandører av KI-systemer utfører for å innhente og gjennomgå erfaringer med bruk av KI-systemer som de bringer i omsetning eller tar i bruk, for det formålet å påvise om det er behov for umiddelbart å iverksette nødvendige korrigerende eller forebyggende tiltak,
- 26) «markedstilsynsmyndighet» den nasjonale myndigheten som utfører aktiviteter og treffer tiltak i samsvar med 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 av tekniske spesifikasjoner som definert i artikkel 2 nr. 4 i forordning (EU) nr. 1025/2012, som gir mulighet for å oppfylle visse krav fastsatt i samsvar med denne forordningen,
- 29) «treningsdata» data som brukes til å trene et KI-system ved å tilpasse dets lærbare parametere,
- 30) «valideringsdata» data som brukes til å gi en evaluering av det trente KI-systemet og justere dets ikke-lærbare parametere og læringsprosess for blant annet å hindre undertilpasning eller overtilpasning,
- 31) «valideringsdatasett» et separat datasett eller en del av treningsdatasettet, enten som en fast eller variabel oppdeling,
- 32) «testdata» data som brukes til å gi en uavhengig evaluering av KI-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 KI-system, og som systemet produserer utdata på grunnlag av,
- 34) «biometriske opplysninger» personopplysninger som stammer fra en særskilt teknisk behandling knyttet til en fysisk persons fysiske, fysiologiske eller atferdsmessige egenskaper, for eksempel ansiktsbilder eller fingeravtrykksopplysninger,
- 35) «biometrisk identifikasjon» automatisk gjenkjenning av fysiske, fysiologiske, atferdsmessige eller psykologiske menneskelige egenskaper med det formålet å fastslå identiteten til en fysisk person ved å sammenligne den personens biometriske opplysninger med biometriske opplysninger om personer lagret i en database,
- 36) «biometrisk verifisering» automatisert en-til-en-verifisering, herunder autentisering, av fysiske personers identitet ved å sammenligne deres biometriske opplysninger med tidligere avgitte biometriske opplysninger,
- 37) «særlige kategorier av personopplysninger» kategoriene av personopplysninger omhandlet 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 data» operasjonelle data om aktiviteter for å forebygge, avsløre, etterforske eller straffeforfølge straffbare forhold som kan sette straffesakers integritet i fare dersom de avsløres,
- 39) «følelsesgjenkjenningssystem» et KI-system som har som formål å identifisere eller utlede fysiske personers følelser eller intensjoner på grunnlag av deres biometriske opplysninger,
- 40) «biometrisk kategoriseringssystem» et KI-system som har som formål å plassere fysiske personer i bestemte kategorier på grunnlag av deres biometriske opplysninger, med mindre det er underordnet en annen kommersiell tjeneste og strengt nødvendig av objektive tekniske årsaker,
- 41) «system for biometrisk fjernidentifikasjon» et KI-system som har som formål å identifisere fysiske personer uten deres aktive medvirkning, vanligvis på avstand, ved å sammenligne en persons biometriske opplysninger med de biometriske opplysningene i en referansedatabase,
- 42) «system for biometrisk fjernidentifikasjon i sanntid» et system for biometrisk fjernidentifikasjon der innhenting av biometriske opplysninger, sammenligningen og identifikasjonen skjer uten vesentlig forsinkelse, som ikke bare omfatter øyeblikkelig identifikasjon, men også begrensede, korte forsinkelser for å unngå omgåelse,
- 43) «system for biometrisk fjernidentifikasjon i ettertid» et system for biometrisk fjernidentifikasjon som ikke er et system for biometrisk fjernidentifikasjon i sanntid,
- 44) «offentlig tilgjengelig sted» ethvert offentlig eid eller privateid fysisk sted som er tilgjengelig for et ubestemt antall fysiske personer, uansett om visse vilkår for tilgang kan gjelde, og uansett de potensielle kapasitetsbegrensningene,

- 45) «rettshåndhevende myndighet»
- a) enhver offentlig myndighet for forebygging, etterforskning, avsløring eller straffeforfølgning av straffbare forhold eller iverksetting av strafferettslige sanksjoner, herunder vern mot og forebygging av trusler mot offentlig sikkerhet,
 - b) ethvert annet organ eller enhver annen enhet som i samsvar med medlemsstatenes nasjonale rett utøver offentlig myndighet og offentlige fullmakter med henblikk på å forebygge, etterforske, avsløre eller straffeforfølge straffbare forhold eller iverksette strafferettslige sanksjoner, herunder vern mot og forebygging av trusler mot offentlig sikkerhet,
- 46) «rettshåndhevelse» aktiviteter utført av rettshåndhevende myndigheter eller på deres vegne for å forebygge, etterforske, avsløre eller straffeforfølge straffbare forhold eller iverksette strafferettslige sanksjoner, herunder vern mot og forebygging av trusler mot offentlig sikkerhet,
- 47) «KI-kontoret» Kommisjonens funksjon med å bidra til gjennomføring og overvåking av og tilsyn med KI-systemer, KI-modeller for allmenne formål, og KI-forvaltning, fastsatt i kommisjonsbeslutning av 24. januar 2024; henvisninger i denne forordningen til KI-kontoret skal forstås som henvisninger til Kommisjonen,
- 48) «nasjonal vedkommende myndighet» en meldermyndighet eller en markedstilsynsmyndighet; når det gjelder KI-systemer som tas i bruk eller brukes av Unionens institusjoner, byråer, kontorer og organer, skal henvisninger i denne forordningen til nasjonale vedkommende myndigheter eller markedstilsynsmyndigheter forstås som henvisninger til EUs datatilsyn,
- 49) «alvorlig hendelse» en hendelse eller funksjonssvikt i et KI-system som direkte eller indirekte fører til
- a) dødsfall eller alvorlig skade på en persons helse,
 - b) en alvorlig og uopprettelig forstyrrelse i forvaltningen eller driften av kritisk infrastruktur,
 - c) overtredelse av forpliktelser i henhold til bestemmelser i unionsretten som har som formål å verne grunnleggende rettigheter,
 - d) alvorlig skade på eiendom eller på miljøet,
- 50) «personopplysninger» personopplysninger som definert i artikkel 4 nr. 1 i forordning (EU) 2016/679,
- 51) «andre data enn personopplysninger» andre data enn personopplysninger som definert i artikkel 4 nr. 1 i forordning (EU) 2016/679,
- 52) «profilering» profilering som definert i artikkel 4 nr. 4 i forordning (EU) 2016/679,
- 53) «plan for testing under virkelige forhold» et dokument som beskriver målene og metoden for, det geografiske, befolkningsmessige og tidsmessige omfanget av samt organiseringen og gjennomføringen av testing under virkelige forhold,
- 54) «sandkasseplan» et dokument avtalt mellom den deltakende leverandøren og vedkommende myndighet som beskriver målene med, vilkårene, tidsrammen og metoden for og kravene til aktivitetene som utføres i sandkassen,
- 55) «regulatorisk sandkasse for KI» en kontrollert ramme opprettet av vedkommende myndighet som gir leverandører eller prospektive leverandører av KI-systemer mulighet til, under virkelige forhold dersom det er relevant, å utvikle, trene, validere og teste et innovativt KI-system i henhold til en sandkasseplan i en begrenset periode under myndighetstilsyn,
- 56) «KI-kompetanse» ferdigheter, kunnskaper og forståelse som gjør det mulig for leverandører, idriftsettere og berørte personer, idet det tas hensyn til deres respektive rettigheter og forpliktelser i forbindelse med denne forordningen, å treffe en informert beslutning om idriftsetting av KI-systemer samt å få bevissthet om mulighetene og risikoene ved KI og hvilken mulig skade det kan forårsake,

- 57) «testing under virkelige forhold» midlertidig testing av et KI-system for dets tiltenkte formål under virkelige forhold som ikke foregår i et laboratorium eller et på annen måte simulert miljø, med sikte på å innhente pålitelige og robuste data og vurdere og verifisere KI-systemets samsvar med kravene i denne forordningen, og som ikke er å anse som å bringe KI-systemet i omsetning eller ta det i bruk i henhold til denne forordningen, forutsatt at alle vilkårene fastsatt i artikkel 57 eller 60 er oppfylt,
- 58) «forsøksperson», i forbindelse med testing under virkelige forhold, en fysisk person som deltar i testing under virkelige forhold,
- 59) «informert samtykke» en forsøkspersons fritt avgitte, spesifikke, utvetydige og frivillige uttrykk for sin vilje til å delta i en bestemt testing under virkelige forhold etter å ha blitt informert om alle sider ved testingen som er relevante for forsøkspersonens beslutning om å delta,
- 60) «dypforfalskning» KI-generert eller -manipulert bilde-, lyd- eller videoinnhold som ligner eksisterende personer, gjenstander, steder, enheter eller hendelser, og som feilaktig kan framstå for en person som autentisk eller sannferdig,
- 61) «utbredt overtredelse» enhver handling eller unnlatelse som er i strid med unionsrettens bestemmelser om vern av enkeltpersoners interesser, og som
- a) har skadet eller kan forventes å skade de kollektive interessene til fysiske personer bosatt i minst to medlemsstater utenom medlemsstaten der
 - i) handlingen eller unnlatelsen har sin opprinnelse eller har funnet sted,
 - ii) den berørte leverandøren eller, dersom det er relevant, dennes bemyndigede representant er lokalisert eller etablert, eller
 - iii) idriftsetteren er etablert, når overtredelsen er begått av idriftsetteren,
 - b) har forårsaket, forårsaker eller kan forventes å forårsake skade på enkeltpersoners kollektive interesser og har felles trekk, herunder at det dreier seg om samme ulovlige praksis, eller at samme interesse krenkes, og begås samtidig av samme operatør i minst tre medlemsstater,
- 62) «kritisk infrastruktur» kritisk infrastruktur som definert i artikkel 2 nr. 4 i direktiv (EU) 2022/2557,
- 63) «KI-modell for allmenne formål» en KI-modell, også dersom den er trent med en stor mengde data ved hjelp av selvovervåking i stor skala, som viser betydelig allmenngyldighet og er i stand til på en kompetent måte å utføre et bredt spekter av særskilte oppgaver uansett hvordan modellen bringes i omsetning, og som kan integreres i en rekke nedstrøms systemer eller applikasjoner, med unntak av KI-modeller som brukes til forsknings-, utviklings- eller prototypingsaktiviteter før de bringes i omsetning,
- 64) «kapabiliteter med høy påvirkningsgrad» kapabiliteter som svarer til eller overgår de kapabilitetene som er registrert i de mest avanserte KI-modellene for allmenne formål,
- 65) «systemrisiko» en risiko som er spesifikk for kapabilitetene med høy påvirkningsgrad i KI-modeller for allmenne formål, og som har betydelig innvirkning på unionsmarkedet på grunn av sin rekkevidde eller på grunn av faktiske eller rimelig forutsigbare negative virkninger på folkehelsen, tryggheten, offentlig sikkerhet, grunnleggende rettigheter eller samfunnet som helhet, og som kan spres i stor skala over hele verdikjeden,
- 66) «KI-system for allmenne formål» et KI-system som er basert på en KI-modell for allmenne formål, og som kan tjene en rekke ulike formål, både ved direkte bruk og ved integrering i andre KI-systemer,
- 67) «flyttallsoperasjon» enhver regneoperasjon eller ligning som involverer flyttall, som er en delmengde av de reelle tallene som på datamaskiner typisk representeres ved et heltall med fast presisjon multiplisert med en heltallsekspONENT med fast grunntall,
- 68) «nedstrømsleverandør» en leverandør av et KI-system, herunder et KI-system for allmenne formål, som integrerer en KI-modell, uansett om KI-modellen leveres av leverandøren selv og integreres vertikalt, eller leveres av en annen enhet på grunnlag av kontraktsforhold.

*Artikkel 4***KI-kompetanse**

Leverandører og idriftsettere av KI-systemer skal treffe tiltak for å sikre, i størst mulig grad, et tilstrekkelig nivå av KI-kompetanse hos sine ansatte og andre personer som arbeider med drift og bruk av KI-systemer på deres vegne, idet det tas hensyn til deres tekniske kunnskap, erfaring, utdanning og opplæring og den sammenhengen KI-systemene skal brukes i, og tatt i betraktning de personene eller gruppene av personer som KI-systemene skal brukes på.

KAPITTEL II

FORBUDT KI-PRAKSIS*Artikkel 5***Forbudt KI-praksis**

1. Følgende former for KI-praksis er forbudt:

- a) Å bringe i omsetning, ta i bruk eller bruke et KI-system som benytter subliminale teknikker utenfor en persons bevissthet, eller bevisst manipulerende eller villedende teknikker, med det formålet eller den virkningen at atferden til en person eller en gruppe personer endres betydelig ved at deres evne til å treffe en informert beslutning blir betraktelig svekket, og dermed får dem til å treffe en beslutning som de ellers ikke ville ha truffet, på en måte som påfører eller med rimelighet kan forventes å påføre den personen, en annen person eller en gruppe personer betydelig skade.
- b) Å bringe i omsetning, ta i bruk eller bruke et KI-system som utnytter noen av sårbarhetene hos en fysisk person eller en bestemt gruppe personer på grunn av alder, nedsatt funksjonsevne eller en bestemt sosial eller økonomisk stilling, med det formålet eller den virkningen at atferden til den personen eller en person som tilhører den gruppen, endres betydelig på en måte som påfører eller med rimelighet kan forventes å påføre den personen eller en annen person betydelig skade.
- c) Å bringe i omsetning, ta i bruk eller bruke KI-systemer for å evaluere eller klassifisere fysiske personer eller grupper av personer over en bestemt tidsperiode basert på deres sosiale atferd eller kjente, utledede eller forutsagte personlige egenskaper eller personlighetstrekk, der den sosiale rangeringen fører til det ene eller begge av følgende:
 - i) skadelig eller ugunstig behandling av visse fysiske personer eller grupper av personer i sosiale sammenhenger som ikke er relatert til de sammenhengene der dataene opprinnelig ble generert eller innhentet,
 - ii) skadelig eller ugunstig behandling av visse fysiske personer eller grupper av personer som er uberettiget eller ikke står i forhold til deres sosiale atferd eller dens alvorlighetsgrad.
- d) Å bringe i omsetning, ta i bruk for dette bestemte formålet eller bruke et KI-system til å gjøre risikovurderinger av fysiske personer for å vurdere eller forutsi risikoen for at en fysisk person begår en straffbar handling, basert utelukkende på profilering av en fysisk person eller vurdering av personens personlighetstrekk og kjennetegn; dette forbudet gjelder ikke KI-systemer som brukes som hjelp til menneskelig vurdering av en persons deltakelse i en kriminell virksomhet, som allerede er basert på objektive og verifiserbare fakta direkte knyttet til en kriminell virksomhet.
- e) Å bringe i omsetning, ta i bruk for dette bestemte formålet eller bruke KI-systemer som oppretter eller utvider ansiktsgjenkjenningsdatabaser gjennom ikke-målrettet skraping av ansiktsbilder fra internett eller overvåkingskameraer.
- f) Å bringe i omsetning, ta i bruk for dette bestemte formålet eller bruke KI-systemer for å tyde fysiske personers følelser på arbeidsplasser og utdanningsinstitusjoner, med mindre bruken av KI-systemet er beregnet på å bli innført eller brakt i omsetning av medisinske eller sikkerhetsmessige årsaker.

- g) Å bringe i omsetning, ta i bruk for dette bestemte formålet eller bruke biometriske kategoriseringssystemer som kategoriserer individuelle fysiske personer basert på deres biometriske opplysninger for å utlede deres rase, politiske meninger, fagforeningsmedlemskap, religiøse eller filosofiske overbevisning, seksuell eller seksuelle legning. Dette forbudet omfatter ikke merking eller filtrering av lovlig ervervede biometriske datasett, for eksempel bilder, basert på biometriske opplysninger, eller kategorisering av biometriske opplysninger på rettshåndhevelsesområdet.
- h) Bruk av systemer for biometrisk fjernidentifikasjon i sanntid på offentlig tilgjengelige steder for rettshåndhevelsesformål, med mindre og i den utstrekning slik bruk er strengt nødvendig for ett av følgende formål:
 - i) målrettet søk etter spesifikke ofre for bortføring, menneskehandel eller seksuell utnyttning av mennesker samt søk etter savnede personer,
 - ii) forebygging av en spesifikk, betydelig og overhengende trussel mot fysiske personers liv eller fysiske sikkerhet eller en reell og tilstedeværende eller reell og forutsigbar trussel om et terrorangrep,
 - iii) lokalisering eller identifikasjon av en person som er mistenkt for å ha begått en straffbar handling, med det formålet å gjennomføre strafferettslig etterforskning eller straffefølgning eller å iverksette en straff for straffbare handlinger som er nevnt i vedlegg II, og som i medlemsstaten det gjelder, kan straffes med fengsel eller et annet frihetsberøvende tiltak med maksimal soningstid på minst fire år.

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

2. Bruk av biometriske fjernidentifikasjonssystemer i sanntid på offentlig tilgjengelige steder med henblikk på rettshåndhevelse for et av formålene nevnt i nr. 1 første ledd bokstav h), skal iverksettes for formålene i nevnte bokstav bare for å bekrefte identiteten til den personen som bruken er spesifikt rettet mot, og det skal tas hensyn til følgende:

- a) karakteren av den situasjonen som gir opphav til den mulige bruken, særlig alvorlighetsgraden av, sannsynligheten for og omfanget av skaden som ville ha oppstått dersom systemet ikke hadde blitt brukt,
- b) de konsekvensene som bruken av systemet får for rettighetene og frihetene til alle berørte personer, særlig alvorlighetsgraden av, sannsynligheten for og omfanget av disse konsekvensene.

Dessuten skal bruk av systemer for biometrisk fjernidentifikasjon i sanntid på offentlig tilgjengelige steder med henblikk på rettshåndhevelse for et av formålene nevnt i nr. 1 første ledd bokstav h) i denne artikkelen skje i samsvar med nødvendige og forholdsmessige sikkerhetstiltak og vilkår i forbindelse med bruken, i samsvar med den nasjonale retten som tillater den, særlig med hensyn til tidsmessige, geografiske og personlige begrensninger. Bruk av systemet for biometrisk fjernidentifikasjon i sanntid på offentlig tilgjengelige steder skal tillates bare dersom den rettshåndhevende myndigheten har foretatt en konsekvensanalyse om grunnleggende rettigheter som fastsatt i artikkel 27 og har registrert systemet i EU-databasen i samsvar med artikkel 49. I behørig begrunnede hastetiltfeller kan imidlertid bruken av slike systemer påbegynnes uten registrering i EU-databasen, forutsatt at registreringen fullføres uten ugrunnet opphold.

3. Ved anvendelse av nr. 1 første ledd bokstav h) og nr. 2 skal det for hver bruk av et system for biometrisk fjernidentifikasjon i sanntid på offentlig tilgjengelige steder med henblikk på rettshåndhevelse kreves en forhåndstillatelse fra en rettsmyndighet eller en uavhengig forvaltningsmyndighet hvis beslutning er bindende for den medlemsstaten der bruken skal skje, utstedt på begrunnet anmodning og i samsvar med de nærmere reglene i nasjonal rett nevnt i nr. 5. I behørig begrunnede hastetiltfeller kan imidlertid bruken av et slikt system påbegynnes uten tillatelse, forutsatt at det anmodes om slik tillatelse uten ugrunnet opphold og senest innen 24 timer. Dersom slik tillatelse nektes, skal bruken umiddelbart bringes til opphør, og alle dataene samt resultatene og utdataene fra denne bruken, skal umiddelbart kasseres og slettes.

Vedkommende rettsmyndighet eller en uavhengig forvaltningsmyndighet hvis beslutning er bindende, skal gi tillatelsen bare dersom den på grunnlag av objektive bevis eller klare indikasjoner som den får seg forelagt, finner det godtgjort at bruken av det aktuelle systemet for biometrisk fjernidentifikasjon i sanntid er nødvendig og forholdsmessig for å oppnå et av målene i nr. 1 første ledd bokstav h), som angitt i anmodningen, og særlig at den forblir begrenset til det som er strengt nødvendig når det gjelder tidsperioden samt det geografiske anvendelsesområdet og de personene som omfattes. Når nevnte myndighet treffer sin beslutning om anmodningen, skal den ta hensyn til faktorene omhandlet i nr. 2. Ingen beslutning som har en negativ rettsvirkning for en person, kan treffes utelukkende på grunnlag av utdataene fra systemet for biometrisk fjernidentifikasjon i sanntid.

4. Uten at det berører nr. 3, skal hver bruk av et system for biometrisk fjernidentifikasjon i sanntid på offentlig tilgjengelige steder for rettshåndhevelsesformål meldes til den relevante markedstilsynsmyndigheten og den nasjonale personvernmyndighe-

ten i samsvar med de nasjonale reglene nevnt i nr. 5. Meldingen skal minst inneholde informasjonen angitt i nr. 6 og skal ikke inneholde sensitive operasjonelle data.

5. En medlemsstat kan beslutte å gi mulighet for helt eller delvis å tillate bruk av systemer for biometrisk fjernidentifikasjon i sanntid på offentlig tilgjengelige steder for rettshåndhevelsesformål, innenfor de grensene og på de vilkårene som er angitt i nr. 1 første ledd bokstav h) og i nr. 2 og 3. De berørte medlemsstatene skal i sin nasjonale rett fastsette de nødvendige nærmere reglene for anmodning om, utstedelse og utøvelse av samt tilsyn med og rapportering om tillatelsene nevnt i nr. 3. I disse reglene skal det også angis for hvilke av formålene i nr. 1 første ledd bokstav h), herunder hvilke av de straffbare handlingene nevnt i bokstav h) iii), vedkommende myndigheter kan tillates å bruke disse systemene for rettshåndhevelsesformål. Medlemsstatene skal meddele disse reglene til Kommisjonen 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. De nasjonale markedstilsynsmyndighetene og de nasjonale personvernmyndighetene i medlemsstater som er blitt underrettet om bruk av systemer for biometrisk fjernidentifikasjon i sanntid på offentlig tilgjengelige steder for rettshåndhevelsesformål i samsvar med nr. 4, skal framlegge årlige rapporter om slik bruk for Kommisjonen. For dette formålet skal Kommisjonen stille en mal til rådighet for medlemsstatene og de nasjonale markedsovervåkings- og personvernmyndighetene som inkluderer informasjon om antallet beslutninger som er truffet av vedkommende rettsmyndigheter eller en uavhengig forvaltningsmyndighet hvis beslutninger er bindende, om anmodninger om tillatelse i samsvar med nr. 3 og resultatet av disse.

7. Kommisjonen skal offentliggjøre årlige rapporter om bruken av systemer for biometrisk fjernidentifikasjon i sanntid på offentlig tilgjengelige steder for rettshåndhevelsesformål, basert på aggregerte data i medlemsstatene som bygger på de årlige rapportene nevnt i nr. 6. Disse årlige rapportene skal ikke inneholde sensitive operasjonelle data om de tilknyttede rettshåndhevelsesaktivitetene.

8. Denne artikkelen berører ikke de forbudene som gjelder dersom en KI-praksis strider mot annen unionsrett.

KAPITTEL III

KI-SYSTEMER MED HØY RISIKO

AVSNITT 1

Klassifisering av KI-systemer som KI-systemer med høy risiko

Artikkel 6

Klassifiseringsregler for KI-systemer med høy risiko

1. Uansett om et KI-system bringes i omsetning eller tas i bruk uavhengig av produktene nevnt i bokstav a) og b), skal det anses som et KI-system med høy risiko dersom begge følgende vilkår er oppfylt:

- a) KI-systemet er beregnet på å brukes som en sikkerhetskomponent i et produkt, eller KI-systemet er i seg selv et produkt som omfattes av EU-harmoniseringsregelverket oppført i vedlegg I.
- b) Produktet hvis sikkerhetskomponent i henhold til bokstav a) er KI-systemet, eller KI-systemet som et produkt i seg selv, må gjennomgå samsvarsvurdering hos en tredjepart for at produktet skal kunne bringes i omsetning eller tas i bruk i samsvar med EU-harmoniseringsregelverket oppført i vedlegg I.

2. I tillegg til de KI-systemene med høy risiko som er nevnt i nr. 1, skal også KI-systemene nevnt i vedlegg III anses som KI-systemer med høy risiko.

3. Som unntak fra nr. 2 skal et KI-system nevnt i vedlegg III ikke anses som et KI-system med høy risiko 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 beslutningsprosesser.

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

- a) KI-systemet er beregnet på å utføre en snever prosedyremessig oppgave.
- b) KI-systemet er beregnet på å forbedre resultatet av en tidligere fullført menneskelig aktivitet.
- c) KI-systemet er beregnet på å finne beslutningsmønstre eller avvik fra tidligere beslutningsmønstre og er ikke beregnet på å erstatte eller påvirke den tidligere fullførte menneskelige vurderingen, uten tilbørlig menneskelig gjennomgang.
- d) KI-systemet er beregnet på å utføre en forberedende oppgave til en vurdering som er relevant for brukstilfellene oppført i vedlegg III.

Uten hensyn til første ledd skal et KI-system nevnt i vedlegg III alltid anses som et KI-system med høy risiko dersom det utfører profilering av fysiske personer.

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

5. Kommisjonen skal etter samråd med Det europeiske rådet for kunstig intelligens («KI-rådet») og senest 2. februar 2026 fastsette retningslinjer for den praktiske gjennomføringen av denne artikkelen i samsvar med artikkel 96 sammen med en omfattende liste over praktiske eksempler på brukstilfeller for KI-systemer med og uten høy risiko.

6. Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 for å endre nr. 3 andre ledd i denne artikkelen 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 KI-systemer som faller inn under virkeområdet for 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 andre ledd i denne artikkelen ved å fjerne ethvert av vilkårene fastsatt der, dersom det foreligger konkrete og pålitelige bevis for at dette er nødvendig for å opprettholde det nivået for vern av helse, sikkerhet og grunnleggende rettigheter som er fastsatt i denne forordningen.

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

Artikkel 7

Endring av vedlegg III

1. Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 for å endre vedlegg III ved å tilføye eller endre brukstilfeller for KI-systemer med høy risiko, dersom begge følgende vilkår er oppfylt:

- a) KI-systemene er beregnet på bruk på et av områdene oppført i vedlegg III.
- b) KI-systemene utgjør en risiko for skade på helse og sikkerhet eller en negativ innvirkning på grunnleggende rettigheter, og denne risikoen tilsvarer eller er større enn risikoen for skade eller negativ innvirkning forbundet med de KI-systemene med høy risiko som allerede er omhandlet i vedlegg III.

2. Når Kommisjonen vurderer vilkåret i nr. 1 bokstav b), skal den ta hensyn til følgende kriterier:

- a) KI-systemets tiltenkte formål.
- b) I hvilken utstrekning et KI-system er blitt brukt eller kan forventes å bli brukt.
- c) Arten og mengden av data som behandles og brukes av KI-systemet, særlig om spesielle kategorier av personopplysninger behandles.
- d) I hvilken utstrekning KI-systemet handler selvstendig, og om det er mulig for et menneske å overstyre en beslutning eller anbefalinger som kan føre til potensiell skade.
- e) I hvilken utstrekning bruken av et KI-system allerede har forårsaket skade på helse og sikkerhet, har hatt en negativ innvirkning på grunnleggende rettigheter eller har skapt betydelig bekymring med hensyn til sannsynligheten for slik skade eller negativ innvirkning, som påvist i for eksempel rapporter eller dokumenterte påstander som er forelagt nasjonale vedkommende myndigheter, eller i andre rapporter, alt etter hva som er relevant.
- f) Det potensielle omfanget av slik skade eller slik negativ innvirkning, særlig med hensyn til dens størrelse og evne til å påvirke flere personer eller til å uforholdsmessig påvirke en bestemt gruppe personer.
- g) I hvilken utstrekning personer som potensielt skades eller rammes av en negativ innvirkning, er avhengige av det resultatet som et KI-system gir, særlig dersom det skyldes at det av praktiske eller juridiske grunner ikke med rimelighet er mulig å velge bort dette resultatet.
- h) I hvilken utstrekning det foreligger en maktubalanse eller personene som potensielt skades eller rammes av en negativ innvirkning, er i en sårbar posisjon i forhold til idriftsetteren av et KI-system, særlig på grunn av status, autoritet, kunnskap, økonomiske eller sosiale omstendigheter eller alder.
- i) I hvilken grad resultatet som produseres ved hjelp av et KI-system, er lett å korrigere eller reversere, tatt i betraktning 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 lette å korrigere eller reversere.
- j) I hvor stor grad og med hvor stor sannsynlighet idriftsettingen av KI-systemet vil være til nytte for enkeltpersoner, grupper eller samfunnet som helhet, herunder mulige forbedringer av produktsikkerheten.
- k) I hvilken utstrekning gjeldende unionsrett fastsetter
 - i) effektive rettsmidler med hensyn til risikoene forbundet med et KI-system, med unntak av erstatningskrav,
 - ii) effektive tiltak for å forebygge eller vesentlig redusere disse risikoene.

3. Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 for å endre vedlegg III ved å fjerne KI-systemer fra listen over KI-systemer med høy risiko dersom begge følgende vilkår er oppfylt:

- a) Det aktuelle KI-systemet utgjør ikke lenger noen vesentlig risiko for grunnleggende rettigheter, helse eller sikkerhet, idet det tas hensyn til kriteriene i nr. 2.
- b) Fjerningen reduserer ikke det generelle nivået for vern av helse, sikkerhet og grunnleggende rettigheter i henhold til unionsretten.

AVSNITT 2

Krav til KI-systemer med høy risiko

Artikkel 8

Oppfyllelse av kravene

1. KI-systemer med høy risiko skal oppfylle kravene fastsatt i dette avsnittet, idet det tas hensyn til deres tiltenkte formål og det allment anerkjente aktuelle tekniske utviklingstrinnet for KI og KI-relaterte teknologier. Det skal tas hensyn til risikostyringssystemet omhandlet i artikkel 9 når det skal sikres at disse kravene oppfylles.

2. Når et produkt inneholder et KI-system som omfattes av kravene i denne forordningen og kravene i EU-harmoniseringsregelverket oppført i avsnitt A i vedlegg I, skal leverandørene ha ansvar for å sikre at produktet fullt ut oppfyller alle gjeldende krav i det gjeldende EU-harmoniseringsregelverket. For å sikre at KI-systemer med høy risiko som nevnt i nr. 1 oppfyller kravene fastsatt i dette avsnittet, og for å sikre konsekvens, unngå dobbeltarbeid og redusere tilleggsbyrdene mest mulig, skal leverandørene når det er hensiktsmessig, kunne velge å integrere de nødvendige test- og rapporteringsprosessene og den nødvendige informasjonen og dokumentasjonen de leverer i forbindelse med sitt produkt, i dokumentasjon og prosedyrer som allerede finnes, og som er påkrevd i henhold til EU-harmoniseringsregelverket oppført i avsnitt A i vedlegg I.

Artikkel 9

Risikohåndteringssystem

1. Et risikohåndteringssystem for KI-systemer med høy risiko skal opprettes, gjennomføres, dokumenteres og vedlikeholdes.
2. Risikohåndteringssystemet skal forstås som en kontinuerlig gjentakende prosess i hele livssyklusen til KI-systemet med høy risiko, som skal gjennomgås og oppdateres systematisk og regelmessig. Det skal omfatte følgende trinn:
 - a) Identifikasjon og analyse av de kjente og rimelig forutsigbare risikoene som KI-systemet med høy risiko kan utgjøre for helse, sikkerhet eller grunnleggende rettigheter når det brukes i samsvar med sitt tiltenkte formål.
 - b) Estimering og evaluering av risikoene som kan oppstå når KI-systemet med høy risiko brukes i samsvar med sitt tiltenkte formål og under forhold med rimelig forutsigbar feilbruk.
 - c) Evaluering av andre risikoer som kan oppstå, på grunnlag av en analyse av data innhentet fra systemet for overvåking etter omsetning omhandlet i artikkel 72.
 - d) Vedtakelse av hensiktsmessige og målrettede risikohåndteringstiltak som er utformet for å håndtere risikoene som identifiseres i samsvar med bokstav a).
3. Risikoene nevnt i denne artikkelen dreier seg bare om slike risikoer som med rimelighet kan reduseres eller fjernes gjennom utviklingen eller utformingen av KI-systemet med høy risiko, eller ved å gi tilfredsstillende teknisk informasjon.
4. Risikohåndteringstiltakene nevnt i nr. 2 bokstav d) skal ta behørig hensyn til virkningene og det mulige samspillet som oppstår når kravene i dette avsnittet anvendes i kombinasjon, med sikte på å minimere risikoene mer effektivt, samtidig som det oppnås en hensiktsmessig balanse ved gjennomføringen av tiltakene for å oppfylle disse kravene.
5. Risikohåndteringstiltakene nevnt i nr. 2 bokstav d) skal være slik at den relevante restrisikoen forbundet med hver fare og den samlede restrisikoen ved KI-systemene med høy risiko anses som akseptabel.

Ved fastsettelse av de mest hensiktsmessige risikohåndteringstiltakene, skal følgende sikres:

- a) Fjerning eller reduksjon av risikoer som er identifisert og vurdert i samsvar med nr. 2, i den grad det er teknisk gjennomførbart gjennom hensiktsmessig utforming og utvikling av KI-systemet med høy risiko.
- b) Dersom det er relevant, gjennomføring av hensiktsmessige avbøtende tiltak og kontrolltiltak mot risikoer som ikke kan fjernes.
- c) At den informasjonen som kreves i samsvar med artikkel 13, stilles til rådighet, og når det er hensiktsmessig, at det gis opplæring til idriftsettere.

For å fjerne eller redusere risikoene knyttet til bruken av KI-systemet med høy risiko skal det tas behørig hensyn til den tekniske kunnskapen, erfaringen, utdanningen og opplæringen som idriftsetteren kan forventes å ha, og den antatte sammenhengen som systemet er ment å brukes i.

6. KI-systemer med høy risiko skal testes med henblikk på å fastslå hva som er de mest hensiktsmessige og målrettede risikohåndteringstiltakene. Testingen skal sikre at KI-systemer med høy risiko fungerer konsekvent for sitt tiltenkte formål, og at de oppfyller kravene i dette avsnittet.
7. Testprosedyrene kan omfatte testing under virkelige forhold i samsvar med artikkel 60.
8. Testing av KI-systemer med høy risiko skal utføres når som helst under utviklingsprosessen, alt etter behov, og under alle omstendigheter før de bringes i omsetning eller tas i bruk. Testingen skal utføres på grunnlag av forhåndsdefinerte mål og sannsynlighetsterskler som er egnet for KI-systemets tiltenkte formål.
9. Når leverandørene gjennomfører risikostyringssystemet som fastsatt i nr. 1–7, skal de ta hensyn til om det er sannsynlig i betraktning av dets tiltenkte formål at KI-systemet med høy risiko vil ha negativ innvirkning på personer under 18 år og, dersom det er relevant, på andre sårbare grupper.
10. For leverandører av KI-systemer med høy risiko som er underlagt krav om interne risikostyringsprosesser i henhold til andre relevante bestemmelser i unionsretten, kan aspektene omhandlet i nr. 1–9 inngå i eller kombineres med risikostyringsprosedyrene fastsatt i samsvar med nevnte bestemmelser.

Artikkel 10

Data og dataforvaltning

1. KI-systemer med høy risiko som benytter teknikker som innebærer trening av KI-modeller med data, skal utvikles på grunnlag av trenings-, validerings- og testdatasett som oppfyller kvalitetskriteriene omhandlet i nr. 2–5, når det brukes slike datasett.
2. Trenings-, validerings- og testdatasett skal være underlagt dataforvaltnings- og datahåndteringsrutiner som er tilpasset KI-systemets tiltenkte formål. Disse rutinene skal særlig dreie seg om
 - a) de relevante utformingsvalgene,
 - b) datainnsamlingsprosesser og opprinnelsen til data, og når det gjelder personopplysninger, det opprinnelige formålet med datainnsamlingen,
 - c) relevante databearbeidingsoperasjoner, for eksempel annotasjon, merking, rensing, oppdatering, foredling og aggregering;
 - d) formulering av antakelser, særlig med hensyn til den informasjonen som dataene skal måle og representere,
 - e) en vurdering av tilgjengeligheten, mengden og egnetheten av de datasettene det er behov for,
 - f) undersøkelse med hensyn til eventuelle skjevheter som kan forventes å påvirke menneskers helse og sikkerhet, ha en negativ innvirkning på grunnleggende rettigheter eller føre til diskriminering som er forbudt etter unionsretten, særlig dersom utdata påvirker inndata til framtidige operasjoner,
 - g) egnede tiltak for å påvise, forebygge og begrense eventuelle skjevheter som er identifisert i samsvar med bokstav f),
 - h) identifikasjon av relevante datahull eller mangler som hindrer overholdelse av denne forordningen, og hvordan disse hullene og manglene kan utbedres.
3. Trenings-, validerings- og testdatasett skal være relevante, tilstrekkelig representative og så vidt mulig feilfrie og fullstendige med tanke på det tiltenkte formålet. De skal ha de hensiktsmessige statistiske egenskapene, herunder eventuelt når det gjelder de personene eller gruppene av personer som KI-systemene med høy risiko er ment å brukes på. Disse egenskapene ved datasettene kan oppfylles for individuelle datasett eller for en kombinasjon av slike.
4. Datasett skal i den grad det tiltenkte formålet krever det, ta hensyn til de kjennetegnene eller elementene som er særegne for de spesifikke geografiske, kontekstuelle, atferdsmessige eller funksjonelle omgivelsene der KI-systemet med høy risiko er ment å brukes.

5. I den utstrekning det er strengt nødvendig for å sikre påvisning og korrigering av skjevheter i forbindelse med KI-systemene med høy risiko i samsvar med nr. 2 bokstav f) og g) i denne artikkelen, kan leverandørene av slike systemer unntaksvis behandle særlige kategorier av personopplysninger, forutsatt at det gis tilstrekkelige garantier for vern av 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 de følgende vilkårene overholdes for at slik behandling skal kunne skje:

- a) Påvisningen og korrigeringen av skjevheter kan ikke fullføres effektivt ved behandling av andre data, herunder syntetiske eller anonymiserte data.
- b) De særlige kategoriene av personopplysninger er omfattet av tekniske begrensninger med hensyn til gjenbruk av personopplysningene samt de mest avanserte sikkerhets- og personverntiltakene, herunder pseudonymisering.
- c) De særlige kategoriene av personopplysninger er omfattet av tiltak for å påse at personopplysningene som behandles, er sikret, beskyttet og underlagt tilfredsstillende garantier, herunder strenge kontroller og dokumentasjon av tilgangen, for å unngå misbruk og sikre at bare autoriserte personer har tilgang til disse personopplysningene, med egnede forpliktelser om fortrolighet,
- d) De særlige kategoriene av personopplysninger blir ikke sendt til, overført til eller på annen måte gjort tilgjengelige for andre parter.
- e) De særlige kategoriene av personopplysninger slettes når skjevheten er korrigert eller når lagringstiden for personopplysningen utløper, avhengig av hva som inntreffer først.
- f) Protokollene over behandlingsaktiviteter i henhold til forordning (EU) 2016/679 og (EU) 2018/1725 og direktiv (EU) 2016/680 inneholder en begrunnelse for hvorfor behandlingen av de særlige kategoriene av personopplysninger var strengt nødvendig for å påvise og korrigere skjevheter, og hvorfor dette målet ikke kunne nås ved behandling av andre data.

6. Ved utvikling av KI-systemer med høy risiko der det benyttes teknikker som omfatter trening av KI-modeller, får nr. 2–5 anvendelse bare på testdatasettene.

Artikkel 11

Teknisk dokumentasjon

1. Den tekniske dokumentasjonen om et KI-system med høy risiko 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 beviser at KI-systemet med høy risiko oppfyller kravene i dette avsnittet, og slik at de nasjonale vedkommende myndighetene og de meldte organene får de opplysningene som er nødvendige for å vurdere om KI-systemet oppfyller disse kravene, i klar og forståelig form. Den skal minst inneholde opplysningene angitt i vedlegg IV. Små og mellomstore bedrifter (SMB-er), herunder oppstartsbedrifter, kan framlegge opplysningene i den tekniske dokumentasjonen angitt i vedlegg IV på en forenklet måte. For dette formålet skal Kommisjonen opprette et forenklet skjema for teknisk dokumentasjon beregnet på å dekke behovene til små og svært små bedrifter. Dersom en SMB, herunder en oppstartsbedrift, velger å gi opplysningene som kreves i henhold til vedlegg IV, på en forenklet måte, skal den bruke skjemaet nevnt i dette nummeret. Meldte organer skal godta skjemaet med henblikk på samsvarsvurderingen.

2. Når et KI-system med høy risiko knyttet til et produkt som omfattes av EU-harmoniseringsregelverket oppført i avsnitt A i vedlegg I, bringes i omsetning eller tas i bruk, skal det utarbeides ett sett med teknisk dokumentasjon som inneholder alle opplysningene angitt 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 å endre vedlegg IV dersom det på grunnlag av den tekniske utviklingen er nødvendig for å sikre at den tekniske dokumentasjonen inneholder alle opplysninger som er nødvendige for å vurdere om systemet oppfyller kravene fastsatt i dette avsnittet.

Artikkel 12

Registrering

1. KI-systemer med høy risiko skal teknisk muliggjøre automatisk registrering av hendelser (logger) i systemets levetid.
2. For å sikre sporbarhet av funksjonen til et KI-system med høy risiko på et nivå som er tilpasset systemets tiltenkte formål, skal loggfunksjonene gjøre det mulig å registrere hendelser som er relevante for å
 - a) påvise situasjoner som kan føre til at KI-systemet med høy risiko utgjør en risiko i henhold til artikkel 79 nr. 1, eller som kan føre til en vesentlig endring,
 - b) lette den overvåkingen etter omsetning som er omhandlet i artikkel 72, og
 - c) overvåke driften av KI-systemer med høy risiko som omhandlet i artikkel 26 nr. 5.
3. For KI-systemer med høy risiko nevnt i nr. 1 bokstav a) i vedlegg III skal loggfunksjonene minst omfatte
 - a) registrering av tidsperioden 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 har ført til treff i søket,
 - d) identifikasjon av de fysiske personene som deltar i kontrollen av resultatene, som omhandlet i artikkel 14 nr. 5.

Artikkel 13

Åpenhet og formidling av opplysninger til idriftsettere

1. KI-systemer med høy risiko skal være utformet og utviklet slik at deres funksjon er tilstrekkelig åpen til at idriftsettere kan tolke et systems utdata og bruke dem på en hensiktsmessig måte. Det skal sikres en hensiktsmessig type og grad av åpenhet for at leverandørene og idriftsetterne skal kunne overholde de relevante forpliktelsene i avsnitt 3.
2. KI-systemer med høy risiko skal ledsages av en bruksanvisning i et egnet digitalt format eller på annen måte som inneholder kortfattet, fullstendig, korrekt og tydelig informasjon som er relevant, tilgjengelig og forståelig for idriftsettere.
3. Bruksanvisningen skal inneholde minst følgende informasjon:
 - a) Identiteten og kontaktopplysningene til leverandøren og eventuelt leverandørens bemyndigede representant.
 - b) Egenskapene, kapabilitetene og ytelsesbegrensningene til KI-systemet med høy risiko, herunder
 - i) dets tiltenkte formål,
 - ii) den nøyaktigheten, herunder målene for den, robustheten og cybersikkerheten, som nevnt i artikkel 15, som KI-systemet med høy risiko er testet og validert mot, og som kan forventes, samt alle kjente og forutsigbare omstendigheter som kan ha innvirkning på denne forventede nøyaktigheten, robustheten og cybersikkerheten,
 - iii) enhver kjent eller forutsigbar omstendighet som er knyttet til bruk av KI-systemet med høy risiko i samsvar med dets tiltenkte formål eller under forhold med rimelig forutsigbar feilbruk, og som kan føre til risiko for helse og sikkerhet eller grunnleggende rettigheter som nevnt i artikkel 9 nr. 2,
 - iv) dersom det er relevant, de tekniske kapabilitetene og egenskapene til KI-systemet med høy risiko når det gjelder å gi informasjon som er relevant for å forklare utdataene fra systemet,

- v) når det er hensiktsmessig, dets ytelse når det gjelder bestemte personer eller grupper av personer som systemet er ment å brukes på,
 - vi) når det er hensiktsmessig, spesifikasjoner for inndataene eller eventuell annen relevant informasjon om de trenings-, validerings- og testdatasettene som brukes, tatt i betraktning det tiltenkte formålet med KI-systemet med høy risiko,
 - vii) dersom det er relevant, informasjon som gjør det mulig for idriftsettere å tolke utdataene fra KI-systemet med høy risiko og bruke dem på en hensiktsmessig måte.
- c) Eventuelle endringer i KI-systemet med høy risiko og dets ytelse som er forhåndsbestemt av leverandøren på tidspunktet for en eventuell innledende samsvarsvurdering.
 - d) Tiltakene for menneskelig tilsyn omhandlet i artikkel 14, herunder de tekniske tiltakene som er innført for å lette idriftsetternes tolkning av utdataene fra KI-systemene med høy risiko.
 - e) Regnekraften og maskinvareressursene som kreves, den forventede levetiden til KI-systemet med høy risiko og eventuelle nødvendige vedlikeholds- og ettersynstiltak, herunder hyppigheten av dem, for å sikre at KI-systemet fungerer som det skal, herunder med hensyn til programvareoppdateringer.
 - f) Dersom det er relevant, en beskrivelse av de mekanismene som inngår i KI-systemet med høy risiko, og som gjør det mulig for idriftsettere å samle inn, lagre og tolke loggene på riktig måte i samsvar med artikkel 12.

Artikkel 14

Menneskelig tilsyn

1. KI-systemer med høy risiko skal utformes og utvikles på en slik måte, herunder med 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 sikte på å forebygge eller minimere risikoene for helse, sikkerhet eller grunnleggende rettigheter som kan oppstå når et KI-system med høy risiko brukes i samsvar med sitt tiltenkte formål eller under forhold med rimelig forutsigbar feilbruk, særlig når slike risikoer vedvarer til tross for anvendelse av andre krav fastsatt i dette avsnittet.
3. Tilsynstiltakene skal stå i forhold til risikoen, graden av autonomi og den sammenhengen KI-systemet brukes i, og skal sikres gjennom en av eller begge følgende typer tiltak:
 - a) Tiltak som leverandøren har identifisert og, når det er teknisk mulig, har bygd inn i KI-systemet med høy risiko før det bringes i omsetning eller tas i bruk.
 - b) Tiltak som leverandøren har identifisert før KI-systemet med høy risiko bringes i omsetning eller tas i bruk, og som er egnet til å gjennomføres av idriftsetteren.
4. Med henblikk på gjennomføringen av nr. 1, 2 og 3 skal KI-systemet med høy risiko leveres til idriftsetteren på en slik måte at fysiske personer som har fått i oppgave å føre menneskelig tilsyn, når det er hensiktsmessig og forholdsmessig, gis mulighet til å
 - a) forstå de relevante funksjonene og begrensningene i KI-systemet på korrekt måte og overvåke driften på behørig vis, blant annet med henblikk på å oppdage og håndtere uregelmessigheter, funksjonsforstyrrelser og uventet ytelse,
 - b) være bevisst på den mulige tendensen til automatisk eller i for høy grad å stole på utdata som produseres av et KI-system med høy risiko (automatiseringsbias), særlig når det gjelder systemer som brukes til å gi informasjon eller anbefalinger i forbindelse med beslutninger som skal tas av fysiske personer,
 - c) tolke utdataene fra KI-systemet på korrekt måte, tatt i betraktning for eksempel de tilgjengelige tolkingsverktøyene og -metodene,

- d) beslutte, i en bestemt situasjon, å ikke bruke KI-systemet eller å se bort fra, overstyre eller reversere systemets utdata på annen måte,
- e) gripe inn i driften av KI-systemet eller avbryte systemet med en stoppknapp eller en lignende prosedyre som gjør at systemet kan stanses i en sikker tilstand.

5. For KI-systemer med høy risiko som nevnt i nr. 1 bokstav a) i vedlegg III skal tiltakene omhandlet i nr. 3 i denne artikkelen dessuten sikre at ingen tiltak eller beslutninger treffes av idriftsetteren på grunnlag av den identifikasjonen som følger av systemet, med mindre identifikasjonen er kontrollert og bekreftet separat av minst to fysiske personer med nødvendig kompetanse, utdanning og myndighet.

Krav om separat verifisering fra minst to fysiske personer skal ikke gjelde for KI-systemer med høy risiko som brukes i forbindelse med rettshåndhevelse, migrasjon, grensekontroll eller asyl, når dette kravet etter unionsretten eller nasjonal rett anses for å være uforholdsmessig.

Artikkel 15

Nøyaktighet, robusthet og cybersikkerhet

1. KI-systemer med høy risiko skal være utformet og utviklet på en slik måte at de oppnår et passende nivå av nøyaktighet, robusthet og cybersikkerhet, og at de yter konsekvent på disse områdene gjennom hele livssyklusen.
2. For å håndtere de tekniske aspektene ved hvordan de passende nivåene av nøyaktighet og robusthet nevnt i nr. 1 og andre relevante ytelsesparametere skal måles, skal Kommisjonen i samarbeid med relevante berørte parter og organisasjoner, for eksempel metrologi- og referansemålingsmyndigheter, oppmuntre til utvikling av referanseverdier og målemetoder når det er relevant.
3. Nøyaktighetsnivåene og de relevante nøyaktighetsparametrene for KI-systemer med høy risiko skal angis i den medfølgende bruksanvisningen.
4. KI-systemer med høy risiko skal være så motstandsdyktige som mulig mot feil, mangler eller uoverensstemmelser som kan oppstå i systemet eller i miljøet der systemet opererer, særlig på grunn av systemets samhandling med fysiske personer eller andre systemer. Det skal treffes tekniske og organisatoriske tiltak for dette formålet.

Robusthet i KI-systemer med høy risiko kan oppnås gjennom tekniske redundansløsninger, som kan omfatte reserveplaner og feilsikringsplaner.

KI-systemer med høy risiko som fortsetter å lære etter at de er brakt i omsetning eller tatt i bruk, skal utvikles på en slik måte at de fjerner eller så langt som mulig reduserer risikoen for skjeve utdata som påvirker innspill til framtidige operasjoner (tilbakemeldingssløyer), og sikrer at eventuelle slike tilbakemeldingssløyer blir håndtert med egnede avbøtende tiltak.

5. KI-systemer med høy risiko skal være motstandsdyktige mot forsøk fra uautoriserte tredjeparter på å endre bruken av systemene eller deres utdata eller ytelse ved å utnytte systemsårbarheter.

De tekniske løsningene som skal ivareta cybersikkerheten i KI-systemer med høy risiko, skal være egnet for de relevante omstendighetene og risikoene.

De tekniske løsningene for å håndtere KI-spesifikke sårbarheter skal, alt etter hva som er relevant, omfatte tiltak for å forebygge, oppdage, respondere på, løse og ta høyde for angrep som forsøker å manipulere treningsdatasett (dataforgiftning) eller forhåndstreinte komponenter som brukes i trainingen (modellforgiftning), inndata som er utformet for å få KI-modellen til å gjøre feil (ondsinnede eksempler eller modellomgåelse), brudd på fortroligheten eller modellfeil.

*AVSNITT 3****Forpliktelser for leverandører og idriftsettere av KI-systemer med høy risiko og for andre parter****Artikkel 16***Forpliktelser for leverandører av KI-systemer med høy risiko**

Leverandører av KI-systemer med høy risiko skal

- a) sikre at deres KI-systemer med høy risiko oppfyller kravene i avsnitt 2,
- b) angi sitt navn, registrerte firmanavn eller registrerte varemerke samt adressen der de kan kontaktes, alt etter hva som er relevant, på KI-systemet med høy risiko eller, dersom dette ikke er mulig, på emballasjen eller i den medfølgende dokumentasjonen,
- c) ha et kvalitetsstyringssystem som er i samsvar med artikkel 17,
- d) oppbevare dokumentasjonen omhandlet i artikkel 18,
- e) når de er under deres kontroll, oppbevare de loggene som automatisk genereres av deres KI-systemer med høy risiko, som omhandlet i artikkel 19,
- f) sikre at KI-systemet med høy risiko gjennomgår den relevante samsvarsvurderingsprosedyren omhandlet i artikkel 43 før det bringes i omsetning eller tas i bruk,
- g) utarbeide en EU-samsvarserklæring i samsvar med artikkel 47,
- h) sette CE-merking på systemet for kunstig intelligens med høy risiko eller, dersom dette ikke er mulig, på emballasjen eller den medfølgende dokumentasjonen for å angi at det er i samsvar med denne forordningen, i samsvar med artikkel 48,
- i) overholde registreringsforpliktelsene nevnt i artikkel 49 nr. 1,
- j) treffe de nødvendige korrigerende tiltakene og framlegge de opplysningene som kreves i henhold til artikkel 20,
- k) etter begrunnet anmodning fra en nasjonal vedkommende myndighet dokumentere at KI-systemet med høy risiko oppfyller kravene i avsnitt 2,
- l) sikre at KI-systemet med høy risiko oppfyller tilgjengelighetskravene i samsvar med direktiv (EU) 2016/2102 og (EU) 2019/882.

*Artikkel 17***Kvalitetsstyringssystem**

1. Leverandører av KI-systemer med høy risiko skal innføre et kvalitetsstyringssystem som sikrer samsvar med denne forordningen. Dette systemet skal dokumenteres på en systematisk og ordnet måte i form av skriftlige retningslinjer, prosedyrer og instruksjoner og skal omfatte minst følgende aspekter:

- a) En strategi for overholdelse av regelverket, herunder overholdelse av prosedyrene for samsvarsvurdering og for styring av endringer i KI-systemet med høy risiko.
- b) Teknikker, prosedyrer og systematiske tiltak som skal brukes ved utforming av KI-systemet med høy risiko og ved kontroll og verifisering av utformingen.
- c) Teknikker, prosedyrer og systematiske tiltak som skal brukes ved utvikling, kvalitetskontroll og kvalitetssikring av KI-systemet med høy risiko.
- d) Undersøkelles-, test- og valideringsprosedyrer som skal utføres før, under og etter utviklingen av KI-systemet med høy risiko, og hyppigheten av dem.

- e) Tekniske spesifikasjoner, herunder standarder, som skal anvendes, og, dersom de relevante harmoniserte standardene ikke anvendes i sin helhet eller ikke dekker alle de relevante kravene i avsnitt 2, de midlene som skal brukes for å sikre at KI-systemet med høy risiko oppfyller disse kravene.
 - f) Systemer og prosedyrer for datahåndtering, herunder datafangst, datainnsamling, dataanalyse, datamerking, datalagring, datafiltrering, datautvinning, dataaggregering, dataoppbevaring og enhver annen operasjon knyttet til dataene som utføres før og med henblikk på omsetning eller ibruktaking av KI-systemer med høy risiko.
 - g) Risikohåndteringssystemet omhandlet i artikkel 9.
 - h) Opprettelse, gjennomføring og vedlikehold av et system for overvåking etter omsetning, i samsvar med artikkel 72.
 - i) Prosedyrer for rapportering av en alvorlig hendelse i samsvar med artikkel 73.
 - j) Håndtering av kommunikasjonen med nasjonale vedkommende myndigheter, andre relevante myndigheter, herunder de som gir eller støtter tilgangen til data, samt meldte organer, andre operatører, kunder eller andre berørte parter.
 - k) Systemer og prosedyrer for registrering av all relevant dokumentasjon og informasjon.
 - l) Ressursforvaltning, herunder tiltak knyttet til forsyningssikkerhet.
 - m) Et rammeverk for ansvarlighet som fastsetter ledelsens og det øvrige personalets ansvar når det gjelder alle aspektene angitt i dette nummeret.
2. Gjennomføringen av aspektene nevnt i nr. 1 skal stå i forhold til størrelsen på leverandørens organisasjon. Leverandørene skal under alle omstendigheter overholde den graden av strenghet og det vernnivået som kreves for å sikre at deres KI-systemer med høy risiko er i samsvar med denne forordningen.
3. Leverandører av KI-systemer med høy risiko som er underlagt forpliktelser med hensyn til kvalitetsstyringssystemer eller en tilsvarende funksjon i henhold til relevant sektorspesifikk unionsrett, kan inkludere aspektene angitt i nr. 1 som en del av de kvalitetsstyringssystemene som er fastsatt i samsvar med nevnte rett.
4. For leverandører som er finansinstitusjoner underlagt krav som gjelder deres interne styreformer, ordninger eller prosesser i henhold til unionsretten om finansielle tjenester, skal plikten til å innføre et kvalitetsstyringssystem, med unntak for nr. 1 bokstav g), h) og i) i denne artikkelen, anses å være oppfylt ved overholdelse av reglene om interne styreformer, ordninger eller prosesser i samsvar med den relevante unionsretten om finansielle tjenester. For dette formålet skal det tas hensyn til eventuelle harmoniserte standarder som omhandlet i artikkel 40.

Artikkel 18

Oppbevaring av dokumentasjon

1. Leverandøren skal i et tidsrom på ti år etter at KI-systemet med høy risiko er brakt i omsetning eller tatt i bruk, kunne stille følgende til rådighet for de nasjonale vedkommende myndighetene:
- a) Den tekniske dokumentasjonen omhandlet i artikkel 11.
 - b) Dokumentasjonen om kvalitetsstyringssystemet omhandlet i artikkel 17.
 - c) Dokumentasjonen for de endringene som er godkjent av meldte organer, dersom det er relevant.
 - d) Beslutningene fra og andre dokumenter som er utstedt av de meldte organene, dersom det er relevant.
 - e) EU-samsvarserklæringen omhandlet i artikkel 47.

2. Hver medlemsstat skal fastsette under hvilke omstendigheter dokumentasjonen nevnt i nr. 1 skal forbli til rådighet for de nasjonale vedkommende myndighetene i tidsrommet angitt i samme nummer, i tilfeller der en leverandør eller dennes bemyndigede representant som er etablert på medlemsstatens territorium, går konkurs eller avslutter sin virksomhet før utgangen av dette tidsrommet.

3. Leverandører som er finansinstitusjoner underlagt krav som gjelder deres interne styreformer, ordninger eller prosesser i henhold til unionsretten om finansielle tjenester, skal oppbevare den tekniske dokumentasjonen som en del av den dokumentasjonen som oppbevares i samsvar med den relevante unionsretten om finansielle tjenester.

Artikkel 19

Automatisk genererte logger

1. Leverandører av KI-systemer med høy risiko skal oppbevare de loggene nevnt i artikkel 12 nr. 1 som automatisk genereres av deres KI-systemer med høy risiko, i den grad disse loggene er under deres kontroll. Uten at det berører gjeldende unionsrett eller nasjonal rett, skal loggene oppbevares i en periode som er egnet ut fra det tiltenkte formålet med KI-systemet med høy risiko, og som er på minst seks måneder, med mindre annet er fastsatt i gjeldende unionsrett eller nasjonal rett, særlig i unionsretten om vern av personopplysninger.

2. Leverandører som er finansinstitusjoner underlagt krav som gjelder deres interne styreformer, ordninger eller prosesser i henhold til unionsretten om finansielle tjenester, skal oppbevare de loggene som automatisk genereres av deres KI-systemer med høy risiko, som en del av den dokumentasjonen som oppbevares i samsvar med den relevante unionsretten om finansielle tjenester.

Artikkel 20

Korrigerende tiltak og opplysningsplikt

1. Leverandører av KI-systemer med høy risiko som mener eller har grunn til å tro at et KI-system med høy risiko som de har brakt i omsetning eller har tatt i bruk, ikke er i samsvar med kravene i denne forordningen, skal umiddelbart treffe de korrigerende tiltakene som er nødvendige for å bringe systemet i samsvar med kravene, trekke det tilbake, deaktivere det eller tilbakekalle det, alt etter hva som er relevant. De skal underrette distributørene av det aktuelle KI-systemet med høy risiko samt, dersom det er relevant, den bemyndigede representanten og importørene om dette.

2. Dersom KI-systemet med høy risiko utgjør en risiko i henhold til artikkel 79 nr. 1 og leverandøren får kjennskap til denne risikoen, skal leverandøren umiddelbart undersøke årsakene, i samarbeid med den rapporterende idriftsetteren dersom det er relevant, og underrette vedkommende markedstilsynsmyndigheter for det aktuelle KI-systemet med høy risiko og, dersom det er relevant, det meldte organet som har utstedt et sertifikat for dette KI-systemet i samsvar med artikkel 44, særlig om arten av den manglende overholdelsen og om eventuelle relevante korrigerende tiltak som er truffet.

Artikkel 21

Samarbeid med vedkommende myndigheter

1. Leverandører av KI-systemer med høy risiko skal på begrunnet anmodning fra vedkommende myndighet gi denne myndigheten all informasjon og dokumentasjon som er nødvendig for å vise at KI-systemet med høy risiko oppfyller kravene i avsnitt 2, på et språk som er lett forståelig for myndigheten, og som er et av de offisielle språkene til Unionens institusjoner, som angitt av den aktuelle medlemsstaten.

2. Etter begrunnet anmodning fra en vedkommende myndighet skal leverandørene dersom det er relevant, også gi den anmodende vedkommende myndigheten tilgang til de automatisk genererte loggene fra KI-systemet med høy risiko som omhandlet i artikkel 12 nr. 1, i den grad disse loggene er under deres kontroll.

3. Alle opplysninger som en vedkommende myndighet får i samsvar med denne artikkelen, skal behandles i samsvar med fortrolighetsforpliktelsene i artikkel 78.

Artikkel 22

Bemyndigede representanter for leverandører av KI-systemer med høy risiko

1. Før de gjør sine KI-systemer med høy risiko tilgjengelige på unionsmarkedet, skal leverandører som er etablert i tredjeland, ved skriftlig fullmakt utpeke en bemyndiget representant som er etablert i Unionen.
2. Leverandøren skal sette sin bemyndigede representant i stand til å utføre de oppgavene som er angitt i fullmakten fra leverandøren.
3. Den bemyndigede representanten skal utføre de oppgavene som er angitt i fullmakten fra leverandøren. Den skal på anmodning framlegge en kopi av fullmakten for markedstilsynsmyndighetene på et av de offisielle språkene til Unionens institusjoner, som angitt av vedkommende myndighet. For denne forordningens formål skal fullmakten gi den bemyndigede representanten myndighet til å utføre følgende oppgaver:
 - a) Verifisere at EU-samsvarserklæringen omhandlet i artikkel 47 og den tekniske dokumentasjonen omhandlet i artikkel 11 er blitt utarbeidet, og, dersom det er relevant, at leverandøren har gjennomført en egnet samsvarsvurderingsprosedyre.
 - b) I et tidsrom på ti år etter at KI-systemet med høy risiko er brakt i omsetning eller tatt i bruk, oppbevare og kunne stille til rådighet for de vedkommende myndighetene og nasjonale myndighetene eller organene som er nevnt i artikkel 74 nr. 10, kontaktopplysningene til den leverandøren som utpekte den bemyndigede representanten, en kopi av EU-samsvarserklæringen nevnt i artikkel 47, den tekniske dokumentasjonen og, dersom det er relevant, sertifikatet utstedt av det meldte organet.
 - c) På begrunnet anmodning gi en vedkommende myndighet alle opplysninger og all dokumentasjon, herunder den som er omhandlet i bokstav b) i dette leddet, som er nødvendig for å påvise at et KI-system med høy risiko oppfyller kravene i avsnitt 2, herunder tilgang til de loggene, som omhandlet i artikkel 12 nr. 1, som automatisk genereres av KI-systemet med høy risiko, i den grad disse loggene er under leverandørens kontroll.
 - d) På begrunnet anmodning samarbeide med vedkommende myndigheter om eventuelle tiltak som sistnevnte treffer i forbindelse med KI-systemet med høy risiko, særlig for å redusere og avbøte risikoene forbundet med KI-systemet med høy risiko.
 - e) Dersom det er relevant, overholde registreringsforpliktelsene nevnt i artikkel 49 nr. 1 eller, dersom registreringen utføres av leverandøren selv, sikre at opplysningene nevnt i vedlegg VIII avsnitt A nr. 3 er korrekte.

Fullmakten skal gi den bemyndigede representanten rett til, i tillegg til eller i stedet for leverandøren, å motta henvendelser fra vedkommende myndigheter i alle spørsmål som gjelder overholdelse av denne forordningen.

4. Den bemyndigede representanten skal si opp fullmakten dersom denne anser eller har grunn til å anta at leverandøren opptrer i strid med sine forpliktelser etter denne forordningen. I så fall skal den bemyndigede representanten umiddelbart underrette den relevante markedstilsynsmyndigheten og, dersom det er relevant, det relevante meldte organet om at fullmakten er oppsagt, og om årsakene til dette.

Artikkel 23

Importørenes forpliktelser

1. Før importører bringer et KI-system med høy risiko i omsetning, skal de sikre at systemet er i samsvar med denne forordningen, ved å verifisere at
 - a) leverandøren av KI-systemet med høy risiko har gjennomført den relevante samsvarsvurderingsprosedyren omhandlet i artikkel 43,
 - b) leverandøren har utarbeidet den tekniske dokumentasjonen i samsvar med artikkel 11 og vedlegg IV,
 - c) systemet har den påkrevde CE-merkingen og ledsages av EU-samsvarserklæringen nevnt i artikkel 47 og bruksanvisningen,
 - d) leverandøren har utpekt en bemyndiget representant i samsvar med artikkel 22 nr. 1.

2. Dersom en importør har tilstrekkelig grunn til å anta at et KI-system med høy risiko ikke er i samsvar med denne forordningen eller er forfalsket eller ledsages av forfalsket dokumentasjon, skal importøren ikke bringe systemet i omsetning før det er brakt i samsvar. Dersom KI-systemet med høy risiko utgjør en risiko i henhold til artikkel 79 nr. 1, skal importøren underrette leverandøren av systemet, den bemyndigede representanten og markedstilsynsmyndighetene om dette.
3. Importører skal angi navn, registrert firmanavn eller registrert varemerke og kontaktadresse på KI-systemet med høy risiko og på dets emballasje eller i den medfølgende dokumentasjonen, dersom det er relevant.
4. Importører skal så lenge de har ansvar for et KI-system med høy risiko, sikre at lagrings- eller transportvilkårene ikke setter dets samsvar med kravene i avsnitt 2 i fare.
5. Importører skal i et tidsrom på ti år etter at KI-systemet med høy risiko er brakt i omsetning eller tatt i bruk, oppbevare en kopi av sertifikatet som er utstedt av det meldte organet, dersom det er relevant, av bruksanvisningen og av EU-samsvarserklæringen omhandlet i artikkel 47.
6. Importørene skal på begrunnet anmodning gi de relevante vedkommende myndighetene all nødvendig informasjon og dokumentasjon, herunder den som er nevnt i nr. 5, for å vise at et KI-systemet med høy risiko oppfyller kravene i avsnitt 2, på et språk som de lett kan forstå. For dette formålet skal de også sikre at den tekniske dokumentasjonen kan gjøres tilgjengelig for disse myndighetene.
7. Importørene skal samarbeide med de relevante vedkommende myndighetene om alle tiltak som disse myndighetene treffer i forbindelse med et KI-system med høy risiko som er brakt i omsetning av importørene, særlig for å redusere og avbøte risikoene forbundet med systemet.

Artikkel 24

Distributørenes forpliktelser

1. Før distributørene gjør et KI-system med høy risiko tilgjengelig på markedet, skal de verifisere at det har den påkrevde CE-merkingen, at det ledsages av et eksemplar av EU-samsvarserklæringen omhandlet i artikkel 47 og en bruksanvisning, og at leverandøren og eventuelt importøren av dette systemet 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 den informasjonen denne er i besittelse av, anser eller har grunn til å anta at et KI-system med høy risiko ikke er i samsvar med kravene i avsnitt 2, skal distributøren ikke gjøre KI-systemet med høy risiko tilgjengelig på markedet før systemet er brakt i samsvar med disse kravene. Dersom KI-systemet med høy risiko utgjør en risiko i henhold til artikkel 79 nr. 1, skal distributøren underrette leverandøren eller importøren av systemet, alt etter hva som er relevant, om dette.
3. Distributører skal så lenge de har ansvar for et KI-system med høy risiko, sikre at lagrings- eller transportvilkårene, dersom det er relevant, ikke setter systemets samsvar med kravene i avsnitt 2 i fare.
4. En distributør som på grunnlag av den informasjonen denne er i besittelse av, anser eller har grunn til å anta et KI-system med høy risiko som distributøren har gjort tilgjengelig på markedet, ikke er i samsvar med kravene i avsnitt 2, skal 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 operatør, avhengig av hva som gjelder, treffer disse korrigerende tiltakene. Dersom KI-systemet med høy risiko utgjør en risiko i henhold til artikkel 79 nr. 1, skal distributøren umiddelbart underrette leverandøren eller importøren av systemet og de myndighetene som er kompetente for det aktuelle KI-systemet, og gi nærmere opplysninger særlig om det manglende samsvaret og eventuelle korrigerende tiltak som er truffet.
5. På begrunnet anmodning fra en relevant vedkommende myndighet skal distributører av et KI-system med høy risiko gi denne myndigheten all den informasjonen og dokumentasjonen om sine tiltak i henhold til nr. 1-4 som er nødvendig for å vise at systemet er i samsvar med kravene i avsnitt 2.
6. Distributørene skal samarbeide med de relevante vedkommende myndighetene om alle tiltak som disse myndighetene treffer i forbindelse med et KI-system med høy risiko som er gjort tilgjengelig på markedet av distributørene, særlig for å redusere eller avbøte risikoen forbundet med systemet.

Artikkel 25

Ansvar langs KI-verdikjeden

1. Enhver distributør, importør, idriftsetter eller annen tredjepart skal ved anvendelsen av denne forordningen anses som leverandør av et KI-system med høy risiko og være underlagt leverandørens forpliktelser i henhold til artikkel 16 under følgende omstendigheter:

- a) De setter sitt navn eller varemerke på et KI-system med høy risiko som allerede er brakt i omsetning eller tatt i bruk, uten at det berører avtalefestede ordninger som fastsetter at forpliktelsene er fordelt annerledes.
- b) De gjør en vesentlig endring av et KI-system med høy risiko som allerede er brakt i omsetning eller allerede er tatt i bruk, på en slik måte at det fortsatt er et KI-system med høy risiko i samsvar med artikkel 6.
- c) De endrer et KI-systems tiltenkte formål, herunder et KI-system for allmenne formål, som ikke er klassifisert som et KI-system med høy risiko, og som allerede er brakt i omsetning eller tatt i bruk, på en slik måte at det aktuelle KI-systemet blir et KI-system med høy risiko i samsvar med artikkel 6.

2. Dersom omstendighetene nevnt i nr. 1 inntreffer, skal den leverandøren som først brakte KI-systemet i omsetning eller tok det i bruk, ikke lenger anses som leverandør av dette spesifikke KI-systemet ved anvendelsen av denne forordningen. Denne første leverandøren skal samarbeide nært med nye leverandører og skal gjøre den nødvendige informasjonen tilgjengelig og gi den tekniske tilgangen som med rimelighet kan forventes, samt annen bistand som kreves for å oppfylle forpliktelsene i denne forordningen, særlig når det gjelder overholdelse av samsvarsvurderingen av KI-systemer med høy risiko. Dette nummeret får ikke anvendelse i tilfeller der den første leverandøren klart har angitt at dennes KI-system ikke skal endres til et KI-system med høy risiko, og derfor ikke omfattes av forpliktelsen til å overlevere dokumentasjonen.

3. Når det gjelder KI-systemer med høy risiko som er sikkerhetskomponenter i produkter omfattet av EU-harmoniseringsregelverket oppført i avsnitt A i vedlegg I, skal produkttilvirkeren anses for å være leverandøren av KI-systemet med høy risiko og være underlagt forpliktelsene i artikkel 16 under følgende omstendigheter:

- a) KI-systemet med høy risiko bringes i omsetning sammen med produktet under produkttilvirkerens navn eller varemerke.
- b) KI-systemet med høy risiko tas i bruk under produkttilvirkerens navn eller varemerke etter at produktet er brakt i omsetning.

4. Leverandøren av et KI-system med høy risiko og tredjeparten som leverer et KI-system, verktøy, tjenester, komponenter eller prosesser som brukes eller integreres i et KI-system med høy risiko, skal ved skriftlig avtale spesifisere informasjonen, kapabilitetene, den tekniske tilgangen og annen bistand som er nødvendig, basert på det allment anerkjente aktuelle tekniske utviklingstrinnet, slik at leverandøren av KI-systemet med høy risiko er i stand til fullt ut å oppfylle forpliktelsene fastsatt i denne forordningen. Dette nummeret får ikke anvendelse på tredjeparter som gjør andre verktøy, tjenester, prosesser eller komponenter enn KI-modeller for allmenne formål tilgjengelige for offentligheten under en lisens med fri og åpen kildekode.

KI-kontoret kan utvikle og anbefale frivillige standardvilkår for avtaler mellom leverandører av KI-systemer med høy risiko og tredjeparter som leverer verktøy, tjenester, komponenter eller prosesser som brukes eller integreres i KI-systemer med høy risiko. Når KI-kontoret utarbeider disse frivillige standardvilkårene, skal det ta hensyn til eventuelle avtalefestede krav som gjelder for bestemte sektorer eller virksomhetsscenarioer. De frivillige standardvilkårene skal offentliggjøres og være tilgjengelige vederlagsfritt i et elektronisk format som er lett å bruke.

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

Artikkel 26

Forpliktelser for idriftsettere av KI-systemer med høy risiko

1. Idriftsettere av KI-systemer med høy risiko skal treffe egnede tekniske og organisatoriske tiltak for å sikre at de bruker disse systemene i samsvar med bruksanvisningen som følger med dem, i samsvar med nr. 3 og 6.

2. Idriftsetterne skal gi oppgaven med å føre menneskelig tilsyn til fysiske personer som har den nødvendige kompetansen, opplæringen og myndigheten samt den nødvendige støtten.
3. Forpliktelsene fastsatt i nr. 1 og 2 berører ikke andre forpliktelser som påhviler idriftsetterne i henhold til unionsretten eller nasjonal rett, eller idriftsetterens frihet til å organisere sine egne ressurser og aktiviteter for det formålet å gjennomføre de tiltakene for menneskelig tilsyn som leverandøren angir.
4. Uten at det berører nr. 1 og 2, skal idriftsetteren, i den grad denne utøver kontroll over inndataene, sikre at inndataene er relevante og tilstrekkelig representative med tanke på KI-systemets tiltenkte formål.
5. Idriftsetterne skal overvåke driften av KI-systemet med høy risiko på grunnlag av bruksanvisningen og, dersom det er relevant, informere leverandørene i samsvar med artikkel 72. Dersom idriftsetterne har grunn til å anta at bruk av KI-systemet med høy risiko i samsvar med bruksanvisningen kan føre til at KI-systemet utgjør en risiko som definert i artikkel 79 nr. 1, skal de uten unødig opphold underrette leverandøren eller distributøren og den relevante markedstilsynsmyndigheten og avbryte bruken av systemet. Dersom idriftsetterne har identifisert en alvorlig hendelse, skal de også umiddelbart underrette først leverandøren og deretter importøren eller distributøren og de relevante markedstilsynsmyndighetene om hendelsen. Dersom idriftsetteren ikke er i stand til å nå leverandøren, skal artikkel 73 gjelde tilsvarende med nødvendige endringer. Denne forpliktelsen omfatter ikke sensitive operasjonelle data tilhørende idriftsettere av KI-systemer som er rettshåndheverende myndigheter.

For idriftsettere som er finansinstitusjoner underlagt krav som gjelder deres interne styreformer, ordninger eller prosesser i henhold til unionsretten om finansielle tjenester, skal overvåkingsplikten fastsatt i første ledd anses å være oppfylt ved overholdelse av reglene om interne styreformer, ordninger, prosesser og mekanismer i samsvar med den relevante retten om finansielle tjenester.

6. Idriftsettere av KI-systemer med høy risiko skal oppbevare loggene som automatisk genereres av disse systemene, i den grad disse loggene er under deres kontroll, i en periode som er egnet ut fra det tiltenkte formålet med KI-systemet med høy risiko, og som er på minst seks måneder, med mindre annet er fastsatt i gjeldende unionsrett eller nasjonal rett, særlig i unionsretten om vern av personopplysninger.

Idriftsettere som er finansinstitusjoner underlagt krav som gjelder deres interne styreformer, ordninger eller prosesser i henhold til unionsretten om finansielle tjenester, skal oppbevare loggene som en del av den dokumentasjonen som oppbevares i samsvar med den relevante unionsretten om finansielle tjenester.

7. Før et KI-system med høy risiko tas i bruk eller brukes på arbeidsplassen, skal idriftsettere som er arbeidsgivere, informere arbeidstakernes representanter og de berørte arbeidstakerne om at de vil bli gjenstand for bruk av KI-systemet med høy risiko. Denne informasjonen skal, dersom det er relevant, gis i samsvar med reglene og prosedyrene fastsatt i Unionens og nasjonal rett og praksis om informasjon til arbeidstakere og deres representanter.
8. Idriftsettere av KI-systemer med høy risiko som er offentlige myndigheter eller Unionens institusjoner, organer, kontorer eller byråer, skal overholde registreringsforpliktelsene omhandlet i artikkel 49. Dersom slike idriftsettere finner at KI-systemet med høy risiko som de vurderer å bruke, ikke er registrert i EU-databasen omhandlet i artikkel 71, skal de avstå fra å bruke dette systemet og underrette leverandøren eller distributøren.
9. Dersom det er relevant, skal idriftsettere av KI-systemer med høy risiko bruke opplysningene som framlegges i samsvar med artikkel 13 i denne forordningen, til å oppfylle sin plikt til å foreta en vurdering av personvernkonsekvenser i samsvar med artikkel 35 i forordning (EU) 2016/679 eller artikkel 27 i direktiv (EU) 2016/680.

10. Uten at det berører direktiv (EU) 2016/680, innenfor rammen av en etterforskning med målrettet søk etter en person som er mistenkt eller dømt for å ha begått en straffbar handling, skal idriftsetteren av et KI-system med høy risiko for biometrisk fjernidentifikasjon i ettertid, på forhånd eller uten unødig opphold og senest innen 48 timer anmode om tillatelse fra en rettsmyndighet eller en forvaltningsmyndighet hvis beslutning er bindende og gjenstand for rettslig prøving, til å bruke dette systemet, unntatt når det brukes til den innledende identifikasjonen av en potensiell mistenkt basert på objektive og verifiserbare fakta som er direkte knyttet til den straffbare handlingen. Hver bruk skal begrenses til det som er strengt nødvendig for etterforskningen av en spesifikk straffbar handling.

Dersom tillatelsen det anmodes om i samsvar med første ledd, blir avslått, skal den bruken av systemet for biometrisk fjernidentifikasjon i ettertid som anmodningen om tillatelse gjelder, stanses med umiddelbar virkning, og personopplysningene knyttet til den bruken av KI-systemet som det ble anmodet om tillatelse til, skal slettes.

Ikke under noen omstendighet skal et slikt KI-system med høy risiko for biometrisk fjernidentifikasjon i ettertid brukes for rettshåndhevelsesformål på en ikke-måltrettet måte, uten noen tilknytning til en straffbar handling, en straffesak, en reell og tilstedeværende eller reell og forutsigbar trussel om en straffbar handling eller et søk etter en bestemt savnet person. Det skal sikres at ingen beslutning som har en negativ rettsvirkning for en person, kan treffes av de rettshåndhevende myndighetene utelukkende på grunnlag av utdataene fra slike systemer for biometrisk fjernidentifikasjon i ettertid.

Dette nummeret berører ikke artikkel 9 i forordning (EU) 2016/679 og artikkel 10 i direktiv (EU) 2016/680 med hensyn til behandling av biometriske opplysninger.

Uavhengig av formål og idriftsetter skal hver bruk av slike KI-systemer med høy risiko dokumenteres i det relevante politiregisteret og stilles til rådighet for den relevante markedstilsynsmyndigheten og den nasjonale personvernmyndigheten på anmodning, unntatt dersom det dreier seg om utlevering av sensitive operasjonelle data knyttet til rettshåndhevelse. Dette leddet berører ikke de fullmaktene som er gitt til tilsynsmyndighetene ved direktiv (EU) 2016/680.

Idriftsetterne skal framlegge årlige rapporter for de relevante markedstilsynsmyndighetene og nasjonale personvernmyndighetene om sin bruk av systemer for biometrisk fjernidentifikasjon i ettertid, unntatt dersom det dreier seg om utlevering av sensitive operasjonelle data knyttet til rettshåndhevelse. Rapportene kan samles for å dekke mer enn én idriftsetting.

Medlemsstatene kan i samsvar med unionsretten innføre mer restriktive lover om bruk av systemer for biometrisk fjernidentifikasjon i ettertid.

11. Uten at det berører artikkel 50 i denne forordningen, skal idriftsettere av KI-systemer med høy risiko omhandlet i vedlegg III som treffer eller bistår i beslutninger som gjelder fysiske personer, informere de fysiske personene om at de er gjenstand for bruk av KI-systemet med høy risiko. Når det gjelder KI-systemer med høy risiko som brukes for rettshåndhevelsesformål, får artikkel 13 i direktiv (EU) 2016/680 anvendelse.

12. Idriftsetterne skal samarbeide med de relevante vedkommende myndighetene i ethvert tiltak som disse myndighetene treffer i forbindelse med KI-systemet med høy risiko for å gjennomføre denne forordningen.

Artikkel 27

Konsekvensanalyse om grunnleggende rettigheter med hensyn til KI-systemer med høy risiko

1. Før de setter i drift et KI-system med høy risiko som nevnt i artikkel 6 nr. 2, med unntak av KI-systemer med høy risiko som er beregnet på å brukes på området nevnt i nr. 2 i vedlegg III, skal idriftsettere som er offentligrettslige organer, eller som er private enheter som yter offentlige tjenester, og idriftsettere av KI-systemer med høy risiko som nevnt nr. 5 bokstav b) og c) i vedlegg III, gjennomføre en vurdering av hvilken innvirkning bruken av et slikt system kan ha på grunnleggende rettigheter. For dette formålet skal idriftsetterne gjennomføre en vurdering bestående av

- a) en beskrivelse av idriftsetterens prosesser der KI-systemet med høy risiko vil bli brukt i samsvar med sitt tiltenkte formål,
- b) en angivelse av hvor lenge og med hvilken hyppighet hvert KI-system med høy risiko er ment å brukes,
- c) de kategoriene av fysiske personer og grupper som kan forventes å bli berørt av bruken av systemet i den spesifikke sammenhengen,
- d) de særlige risikoene for skade som kan forventes å ha innvirkning på de kategoriene av fysiske personer eller grupper av personer som identifiseres i henhold til bokstav c) i dette nummeret, idet det tas hensyn til opplysningene som framlegges av leverandøren i samsvar med artikkel 13,
- e) en beskrivelse av gjennomføringen av tiltak for menneskelig tilsyn, i samsvar med bruksanvisningen.
- f) tiltakene som skal treffes i tilfelle disse risikoene oppstår, herunder de interne styreformene og klageordningene.

2. Forpliktelsen fastsatt i nr. 1 gjelder for første gangs bruk av KI-systemet med høy risiko. I lignende tilfeller kan idriftsetteren vise til tidligere gjennomførte konsekvensanalyser om grunnleggende rettigheter eller eksisterende konsekvensanalyser gjennomført av leverandøren. Dersom idriftsetteren under bruk av KI-systemet med høy risiko finner at noen av opplysningene oppført i nr. 1 har endret seg eller ikke lenger er oppdatert, skal idriftsetteren treffe de nødvendige tiltakene for å oppdatere opplysningene.
3. Når analysen omhandlet i nr. 1 i denne artikkelen er gjennomført, skal idriftsetteren underrette markedstilsynsmyndigheten om resultatene av analysen og sende inn den utfylte malen nevnt i nr. 5 i denne artikkelen som en del av underretningen. I tilfellet omhandlet i artikkel 46 nr. 1 kan idriftsettere fritas fra denne underretningsplikten.
4. Dersom noen av forpliktelsene fastsatt i denne artikkelen allerede er oppfylt gjennom vurderingen av personvernkonsekvenser gjennomført i henhold til artikkel 35 i forordning (EU) 2016/679 eller artikkel 27 i direktiv (EU) 2016/680, skal konsekvensanalysen om grunnleggende rettigheter omhandlet i nr. 1 i denne artikkelen supplere vurderingen av personvernkonsekvenser.
5. KI-kontoret skal utarbeide en mal for et spørreskjema, herunder gjennom et automatisert verktøy, for å gjøre det lettere for idriftsettere å overholde sine forpliktelser i henhold til denne artikkelen.

AVSNITT 4

Meldermyndigheter og meldte organer

Artikkel 28

Meldermyndigheter

1. Hver medlemsstat skal utpeke eller opprette minst én meldermyndighet som er ansvarlig for å etablere og gjennomføre de nødvendige prosedyrene for vurdering, utpeking og melding av samsvarsvurderingsorganer og for tilsynet med dem. Disse prosedyrene skal utarbeides i samarbeid mellom meldermyndighetene i alle medlemsstater.
2. Medlemsstatene kan beslutte at vurdering og tilsyn som nevnt i nr. 1 skal utføres av et nasjonalt akkrediteringsorgan slik det er definert i forordning (EF) nr. 765/2008, og i samsvar med den forordningen.
3. Meldermyndigheter skal opprettes, organiseres og drives på en slik måte at det ikke oppstår interessekonflikter med samsvarsvurderingsorganer, og sikres at deres virksomhet er objektiv og upartisk.
4. Meldermyndigheter skal være organisert på en slik måte at beslutninger om melding av et samsvarsvurderingsorgan treffes av kvalifiserte personer som er noen andre enn dem som har utført vurderingen av disse organene.
5. Meldermyndigheter skal ikke tilby eller utøve noen virksomhet som samsvarsvurderingsorganer utøver, eller yte noen rådgivningstjenester på forretningsmessig eller konkurransemessig grunnlag.
6. Meldermyndigheter skal sikre at opplysningene de innhenter, behandles fortrolig, i samsvar med artikkel 78.
7. Meldermyndigheter skal ha et tilstrekkelig stort kvalifisert personale til å kunne utføre sine oppgaver på en tilfredsstillende måte. Det kvalifiserte personalet skal, dersom det er relevant, ha den nødvendige fagkunnskapen for sin funksjon på områder som informasjonsteknologi, kunstig intelligens og juss, herunder tilsyn med grunnleggende rettigheter.

Artikkel 29

Søknad om melding fra et samsvarsvurderingsorgan

1. Samsvarsvurderingsorganer skal inngi en søknad om melding til meldermyndigheten i den medlemsstaten der de er etablert.

2. Søknaden om melding skal ledsages av en beskrivelse av de samsvarsvurderingsaktivitetene, den eller de samsvarsvurderingsmodulene og de typene av KI-systemer som samsvarsvurderingsorganet hevder å være kompetent for, samt eventuelt et akkrediteringsbevis utstedt av et nasjonalt akkrediteringsorgan som bekrefter at samsvarsvurderingsorganet oppfyller kravene fastsatt i artikkel 31.

Ethvert gyldig dokument knyttet til eksisterende utpekinger i henhold til annet EU-harmoniseringsregelverk av det organet som søker om å bli meldt, skal tilføyes.

3. Dersom samsvarsvurderingsorganet ikke kan framlegge et akkrediteringsbevis, skal det gi meldermyndigheten all dokumentasjon som er nødvendig for å verifisere, anerkjenne og føre regelmessig tilsyn med at organet oppfyller kravene fastsatt i artikkel 31.

4. For meldte organer som er utpekt i henhold til annet EU-harmoniseringsregelverk, kan alle dokumenter og sertifikater som er knyttet til disse utpekingene, eventuelt brukes til støtte for utpekingsprosedyren fastsatt i denne forordningen. Det meldte organet skal oppdatere dokumentasjonen nevnt i nr. 2 og 3 når det skjer relevante endringer, slik at myndigheten med ansvar for meldte organer kan føre tilsyn med og kontrollere at alle kravene fastsatt i artikkel 31 fortsatt er oppfylt.

Artikkel 30

Meldingsprosedyre

1. Meldermyndighetene kan bare melde samsvarsvurderingsorganer som oppfyller kravene i artikkel 31.
2. Meldermyndighetene skal melde hvert samsvarsvurderingsorgan som nevnt i nr. 1 til Kommisjonen og de andre medlemsstatene ved hjelp av det elektroniske meldingsverktøyet som Kommisjonen har utviklet og forvalter.
3. Meldingen nevnt i nr. 2 i denne artikkelen skal inneholde fullstendige opplysninger om samsvarsvurderingsaktivitetene, samsvarsvurderingsmodulen eller -modulene og de aktuelle typene av KI-systemer, samt relevant attestasjon på kompetanse. Dersom en melding ikke bygger på et akkrediteringsbevis som omhandlet i artikkel 29 nr. 2, skal meldermyndigheten gi Kommisjonen og de andre medlemsstatene dokumentasjon som bekrefter samsvarsvurderingsorganets kompetanse og de ordningene som er innført for å sikre at det vil bli ført regelmessig tilsyn med organet, og at organet fortsatt vil oppfylle kravene i artikkel 31.
4. Samsvarsvurderingsorganet det gjelder, kan utøve virksomhet som meldt organ bare dersom Kommisjonen eller de andre medlemsstatene ikke har gjort innsigelser mot dette innen to uker etter en melding fra en meldermyndighet som inneholder et akkrediteringsbevis som omhandlet i artikkel 29 nr. 2, eller innen to måneder etter en melding fra en meldermyndighet som inneholder dokumentasjon som omhandlet i artikkel 29 nr. 3.
5. Dersom det gjøres innsigelser, skal Kommisjonen umiddelbart innlede samråd med medlemsstatene det gjelder, og samsvarsvurderingsorganet. På grunnlag av dette skal Kommisjonen beslutte om tillatelsen er berettiget. Kommisjonen skal rette sin beslutning til medlemsstaten det gjelder, og til det relevante samsvarsvurderingsorganet.

Artikkel 31

Krav til meldte organer

1. Et meldt organ skal opprettes i henhold til en medlemsstats nasjonale rett og skal være et rettssubjekt.
2. Meldte organer skal oppfylle de organisatoriske kravene og de kravene til kvalitetsstyring, ressurser og prosesser som er nødvendige for at de skal kunne utføre sine oppgaver, samt egnede cybersikkerhetskrav.
3. Meldte organers organisasjonsstruktur, ansvarsfordeling, rapporteringslinjer og drift skal sikre tillit til deres arbeid og til resultatene av de samsvarsvurderingsaktivitetene de utfører.

4. Meldte organer skal være uavhengige av leverandøren av et KI-system med høy risiko som er gjenstand for deres samsvarsvurderingsaktiviteter. Meldte organer skal også være uavhengige av enhver annen operatør med interesse i det KI-systemet med høy risiko som vurderes, samt av eventuelle konkurrenter til leverandøren. Dette skal ikke hindre bruk av vurderte KI-systemer med høy risiko som er nødvendige for samsvarsvurderingsorganets virksomhet, eller bruk av slike systemer KI-systemer med høy risiko for personlige formål.
5. Verken et samsvarsvurderingsorgan, dets øverste ledelse eller personalet med ansvar for å utføre samsvarsvurderingsoppgavene skal være direkte involvert i utvikling, produksjon, markedsføring eller bruk av KI-systemer med høy risiko eller representere partene som deltar i disse aktivitetene. De skal ikke delta i noen virksomhet som kan være i strid med deres uavhengighet eller integritet i forbindelse med samsvarsvurderingsaktivitetene de er meldt for. Dette gjelder særlig rådgivningstjenester.
6. Meldte organer skal organiseres og drives på en måte som sikrer at deres virksomhet er uavhengig, objektiv og upartisk. Meldte organer skal dokumentere og gjennomføre en struktur og prosedyrer for å sikre upartiskhet og for å fremme og anvende prinsippene for upartiskhet i hele organisasjonen, blant alt personale og i all vurderingsvirksomhet.
7. Meldte organer skal ha innført dokumenterte prosedyrer som sikrer at deres personale, utvalg, datterforetak, underleverandører og eventuelle tilknyttede organer eller personale i eksterne organer, i samsvar med artikkel 78 bevarer fortrolighet om den informasjonen de kommer i besittelse av i forbindelse med samsvarsvurderingsaktiviteter, med mindre utlevering av informasjonen er påbudt ved lov. Meldte organers personale skal være underlagt taushetsplikt med hensyn til all informasjon som de kommer i besittelse av når de utfører sine oppgaver i samsvar med denne forordningen, unntatt overfor meldermyndighetene i den medlemsstaten der virksomheten utføres.
8. Meldte organer skal ha prosedyrer for utøvelse av virksomhet som tar behørig hensyn til leverandørens størrelse, sektoren der den driver sin virksomhet, og dens struktur, samt kompleksiteten av det aktuelle KI-systemet.
9. Meldte organer skal tegne en egnet ansvarsforsikring for sine samsvarsvurderingsaktiviteter med mindre medlemsstaten der de er etablert, påtar seg erstatningsansvaret i samsvar med nasjonal rett, eller medlemsstaten selv er direkte ansvarlig for samsvarsvurderingen.
10. Meldte organer skal være i stand til å utføre alle sine oppgaver i henhold til denne forordningen med største mulige faglige integritet og med den nødvendige kompetansen på det spesifikke området, enten oppgavene utføres av de meldte organene selv eller på deres vegne og under deres ansvar.
11. Meldte organer skal ha tilstrekkelig intern kompetanse til effektivt å kunne evaluere de oppgavene som utføres av eksterne parter på deres vegne. Det meldte organet skal ha permanent tilgang til tilstrekkelig med administrativt, teknisk, juridisk og vitenskapelig personale som har erfaring med og kunnskap om de relevante typene av KI-systemer, data og databehandling samt om kravene i avsnitt 2.
12. Meldte organer skal delta i samordningen omhandlet i artikkel 38. De skal også delta direkte eller være representert i europeiske standardiseringsorganisasjoner eller sørge for å holde seg orientert om relevante standarder.

Artikkel 32

Formodning om samsvar med krav til meldte organer

Dersom et samsvarsvurderingsorgan dokumenterer at det overholder kriteriene fastsatt i relevante harmoniserte standarder eller deler av disse som det er offentliggjort henvisninger til i *Den europeiske unions tidende*, skal det formodes å oppfylle kravene i artikkel 31 i den grad de gjeldende harmoniserte standardene omfatter nevnte krav.

Artikkel 33

Datterforetak til meldte organer og underleveranser

1. Dersom et meldt organ overlater bestemte oppgaver i forbindelse med samsvarsvurderingen til en underleverandør eller 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 påta seg det fulle ansvaret for de oppgavene som utføres av underleverandører eller datterforetak.
3. Oppgaver kan bare overlates til en underleverandør eller et datterforetak med leverandørens samtykke. Meldte organer skal offentliggjøre en liste over sine datterforetak.
4. De relevante dokumentene om vurderingen av underleverandørens eller datterforetakets kvalifikasjoner og arbeidet de har utført i henhold til denne forordningen, skal holdes tilgjengelige for meldermyndigheten i fem år fra det tidspunktet underleveransen opphører.

Artikkel 34

Meldte organers driftsmessige forpliktelser

1. Meldte organer skal verifisere at KI-systemer med høy risiko er i samsvar med kravene, i henhold til samsvarsvurderingsprosedyrene fastsatt i artikkel 43.
2. Meldte organer skal unngå unødvendige byrder for leverandører under utøvelsen av sin virksomhet og ta behørig hensyn til leverandørens størrelse, i hvilken sektor den driver sin virksomhet, og dens struktur, samt kompleksiteten av det aktuelle KI-systemet med høy risiko, særlig for å minimere administrative byrder og etterlevelseskostnader for svært små og små bedrifter som definert i rekommandasjon 2003/361/EF. Det meldte organet skal likevel overholde den graden av strenghet og det vernnivået som kreves for at KI-systemet med høy risiko skal være i samsvar med kravene i denne forordningen.
3. Meldte organer skal gjøre tilgjengelig og på anmodning framlegge all relevant dokumentasjon, herunder leverandørens dokumentasjon, for meldermyndigheten omhandlet i artikkel 28, slik at denne kan utøve sin vurderings-, utpekings-, meldings-, og tilsynsvirksomhet, og for å lette vurderingen omhandlet i dette avsnittet.

Artikkel 35

Identifikasjonsnumre og lister over meldte organer

1. Kommisjonen skal tildele hvert meldt organ bare ett identifikasjonsnummer, selv om et organ er meldt i henhold til mer enn én unionsrettsakt.
2. Kommisjonen skal offentliggjøre listen over organene som er meldt i henhold til denne forordningen, herunder deres identifikasjonsnummer og virksomheten de er meldt for. Kommisjonen skal sørge for at listen holdes oppdatert.

Artikkel 36

Endring av meldinger

1. Meldermyndigheten skal underrette Kommisjonen og de andre medlemsstatene om eventuelle relevante endringer i meldingen av et meldt organ, via det elektroniske meldingsverktøyet nevnt i artikkel 30 nr. 2.
2. Prosedyrene fastsatt i artikkel 29 og 30 får anvendelse ved utvidelser av meldingens omfang.

Ved andre endringer av meldingen enn utvidelser av dens omfang får prosedyrene fastsatt i nr. 3–9 anvendelse.

3. Dersom et meldt organ beslutter å innstille sine samsvarsvurderingsaktiviteter, skal det underrette meldermyndigheten og de berørte leverandørene så snart som mulig og, dersom innstillingen er planlagt, minst ett år før virksomheten innstilles. Det meldte organets sertifikater kan forbli gyldige i ni måneder etter at det meldte organets virksomhet er innstilt, forutsatt at et annet meldt organ skriftlig har bekreftet at det vil påta seg ansvaret for de KI-systemene med høy risiko som omfattes av disse sertifikatene. Sistnevnte meldte organ skal foreta en fullstendig vurdering av de aktuelle KI-systemene med høy risiko innen utgangen av denne nīmānedersperioden før det utsteder nye sertifikater for disse systemene. Dersom det meldte organet har innstilt sin virksomhet, skal meldermyndigheten trekke tilbake utpekingen.
4. Dersom meldermyndigheten har tilstrekkelig grunn til å anta at et meldt organ ikke lenger oppfyller kravene i artikkel 31, eller at det unnlater å oppfylle sine forpliktelser, skal den umiddelbart undersøke saken med den største omhyggelighet. I den forbindelse skal den underrette det aktuelle meldte organet om innsigelsene som er gjort, og gi det mulighet til å uttale seg. Dersom meldermyndigheten kommer til den konklusjonen at det meldte organet ikke lenger oppfyller kravene fastsatt i artikkel 31, eller at det unnlater å oppfylle sine forpliktelser, skal den enten begrense, suspendere eller trekke tilbake utpekingen, alt etter hvor alvorlig den manglende overholdelsen av disse kravene eller forpliktelsene er. Den skal umiddelbart underrette Kommisjonen og de andre medlemsstatene om dette.
5. Dersom utpekingen av et meldt organ er blitt suspendert, begrenset eller helt eller delvis trukket tilbake, skal det meldte organet underrette de berørte leverandørene om dette innen ti dager.
6. I tilfelle av begrensning, suspensjon eller tilbaketrekking av en utpeking skal meldermyndigheten treffe egnede tiltak for å sikre at det berørte meldte organets dokumenter bevares, og for å gjøre dem tilgjengelige for meldermyndighetene i andre medlemsstater og for markedstilsynsmyndighetene på deres anmodning.
7. I tilfelle av begrensning, suspensjon eller tilbaketrekking av en en utpeking skal meldermyndigheten
 - a) vurdere hvilken innvirkning dette får på sertifikatene som er utstedt av det meldte organet,
 - b) framlegge en rapport om sine konklusjoner for Kommisjonen og de andre medlemsstatene senest tre måneder etter at den har meldt endringen av utpekingen,
 - c) kreve at det meldte organet innen en rimelig frist som fastsettes av myndigheten, suspenderer eller trekker tilbake eventuelle sertifikater som er urettmessig utstedt, for å sikre at KI-systemer med høy risiko som finnes på markedet, fortsatt er i samsvar med kravene,
 - d) underrette Kommisjonen og medlemsstatene om sertifikater som den har krevd suspensjon eller tilbaketrekking av,
 - e) gi den nasjonale vedkommende myndigheten i medlemsstaten der leverandøren har sitt registrerte forretningssted, alle relevante opplysninger om de sertifikatene den har krevd suspensjon eller tilbaketrekking av; nevnte myndighet skal om nødvendig treffe egnede tiltak for å unngå potensiell risiko for helse, sikkerhet eller grunnleggende rettigheter.
8. Med unntak av urettmessig utstedte sertifikater og tilfeller der en utpeking er blitt suspendert eller begrenset, skal sertifikater forbli gyldige dersom
 - a) meldermyndigheten senest en måned etter suspensjonen eller begrensningen har bekreftet at det ikke er noen risiko for helse, sikkerhet eller grunnleggende rettigheter forbundet med sertifikater som omfattes av suspensjonen eller begrensningen, og meldermyndigheten har angitt en frist for tiltak beregnet på avhjelpe suspensjonen eller begrensningen, eller
 - b) meldermyndigheten har bekreftet at ingen sertifikater som omfattes av suspensjonen, vil bli utstedt, endret eller utstedt på nytt så lenge suspensjonen eller begrensningen varer, og angir om det meldte organet har kapasitet til å fortsette å føre tilsyn med og ha ansvar for eksisterende sertifikater som er utstedt for den perioden som suspensjonen eller begrensningen gjelder; dersom meldermyndigheten finner at det meldte organet ikke har kapasitet til å opprettholde eksisterende utstedte sertifikater, skal leverandøren av det systemet som omfattes av sertifikatet, senest tre måneder etter suspensjonen eller begrensningen skriftlig bekrefte overfor de nasjonale vedkommende myndighetene i medlemsstaten der den har sitt registrerte forretningssted, at et annet kvalifisert meldt organ midlertidig påtar seg det meldte organets oppgaver med å føre tilsyn med og ha ansvar for sertifikatene i den perioden som suspensjonen eller begrensningen gjelder.

9. Med unntak av urettmessig utstedte sertifikater og tilfeller der en utpeking er trukket tilbake, skal sertifikatene forbli gyldige i ni måneder dersom

- a) vedkommende nasjonale myndighet i den medlemsstaten der leverandøren av de KI-systemene med høy risiko som omfattes av sertifikatet, har sitt registrerte forretningssted, har bekreftet at det ikke er noen risiko for helse, sikkerhet eller grunnleggende rettigheter forbundet med nevnte KI-systemer med høy risiko, og
- b) et annet meldt organ skriftlig har bekreftet at det umiddelbart vil påta seg ansvaret for nevnte KI-systemer med høy risiko og fullføre sin vurdering innen tolv måneder etter at utpekingen er trukket tilbake.

Under omstendighetene omhandlet i første ledd kan den nasjonale vedkommende myndigheten i den medlemsstaten der leverandøren av systemet som omfattes av sertifikatet, har sitt forretningssted, forlenge sertifikatenes midlertidige gyldighet i ytterligere perioder på tre måneder, som til sammen ikke skal overstige tolv måneder.

Den nasjonale vedkommende myndigheten eller det meldte organet som påtar seg oppgavene til det meldte organet som er berørt av endringen av utpekingen, skal umiddelbart underrette Kommisjonen, de andre medlemsstatene og de andre meldte organene om dette.

Artikkel 37

Tvil om meldte organers kompetanse

1. Kommisjonen skal om nødvendig undersøke alle tilfeller der det er grunn til å tvile på at et meldt organ er kompetent eller fortsatt oppfyller kravene fastsatt i artikkel 31 og ivaretar det ansvaret det er pålagt.
2. Meldermyndigheten skal på anmodning gi Kommisjonen alle relevante opplysninger i forbindelse med meldingen eller opprettholdelsen av det aktuelle meldte organets kompetanse.
3. Kommisjonen skal sikre at alle sensitive opplysninger som den innhenter under sine undersøkelser, blir behandlet fortrolig i samsvar med artikkel 78.
4. Dersom Kommisjonen fastslår at et meldt organ ikke oppfyller eller ikke lenger oppfyller kravene som gjelder for meldingen, skal den underrette meldermedlemsstaten om dette og anmode den om å treffe de nødvendige korrigerende tiltakene, herunder om nødvendig suspensjon eller tilbaketrekking av meldingen. Dersom medlemsstaten ikke treffer de nødvendige korrigerende tiltakene, kan Kommisjonen ved hjelp av en gjennomføringsrettsakt suspendere, begrense eller trekke tilbake utpekingen. Denne gjennomføringsrettsakten skal vedtas i samsvar med undersøkelsesprosedyren nevnt i artikkel 98 nr. 2.

Artikkel 38

Samordning av meldte organer

1. Kommisjonen skal sørge for, når det gjelder KI-systemer med høy risiko, at det innføres egnet samordning av og samarbeid mellom meldte organer som deltar i prosedyrene for samsvarsvurdering i henhold til denne forordningen, og at dette forvaltes på en hensiktsmessig måte i form av en sektorspesifikk gruppe av meldte organer.
2. Hver meldermyndighet skal sørge for at de organene den har meldt, deltar i arbeidet til gruppen nevnt i nr. 1, enten direkte eller gjennom utpekte representanter.
3. Kommisjonen skal sørge for utveksling av kunnskap og beste praksis mellom meldermyndighetene.

Artikkel 39

Samsvarsvurderingsorganer i tredjeland

Samsvarsvurderingsorganer som er opprettet i henhold til retten i et tredjeland som Unionen har inngått avtale med, kan gis tillatelse til å utføre aktivitetene til meldte organer i henhold til denne forordningen, forutsatt at de oppfyller kravene i artikkel 31, eller at de sikrer et tilsvarende nivå av samsvar.

AVSNITT 5

Standarder, samsvarsvurdering, sertifikater, registrering

Artikkel 40

Harmoniserte standarder og standardiseringspublikasjoner

1. KI-systemer med høy risiko eller KI-modeller for allmenne formål som er i samsvar med harmoniserte standarder, eller deler av slike, som det er offentliggjort henvisninger til i *Den europeiske unions tidende* i samsvar med forordning (EU) nr. 1025/2012, skal formodes å oppfylle kravene i avsnitt 2 i dette kapitlet eller, dersom det er relevant, forpliktelsene i kapittel V avsnitt 2 og 3 i denne forordningen, i den grad disse standardene omfatter nevnte krav eller forpliktelser.

2. I samsvar med artikkel 10 i forordning (EU) nr. 1025/2012 skal Kommisjonen uten ugrunnet opphold utstede anmodninger om standardisering som omfatter alle kravene i avsnitt 2 i dette kapitlet, og, dersom det er relevant, anmodninger om standardisering som omfatter forpliktelser i kapittel V avsnitt 2 og 3 i denne forordningen. I anmodningen om standardisering skal det også anmodes om publikasjoner om rapporterings- og dokumentasjonsprosesser for å forbedre KI-systemers ressursytelse, for eksempel å redusere forbruket av energi og andre ressurser hos KI-systemet med høy risiko under dets livssyklus, samt om energieffektiv utvikling av KI-modeller for allmenne formål. Når Kommisjonen utarbeider en anmodning om standardisering, skal den rådspørre KI-rådet og relevante berørte parter, herunder det rådgivende forumet.

Når Kommisjonen utsteder en anmodning om standardisering til europeiske standardiseringsorganisasjoner, skal den angi at standardene må være klare og konsekvente, også med standardene utarbeidet i de ulike sektorene for produkter som omfattes av det eksisterende EU-harmoniseringsregelverket oppført i vedlegg I, og ha som mål å sikre at KI-systemer med høy risiko eller KI-modeller for allmenne formål som bringes i omsetning eller tas i bruk i Unionen, oppfyller de relevante kravene eller forpliktelsene fastsatt i denne forordningen.

Kommisjonen skal anmode de europeiske standardiseringsorganisasjonene om å framlegge dokumentasjon på at de har gjort sitt ytterste for å oppfylle målene nevnt i første og andre ledd i dette nummeret i samsvar med artikkel 24 i forordning (EU) nr. 1025/2012.

3. Deltakerne i standardiseringsprosessen skal søke å fremme investeringer og innovasjon i KI, blant annet ved å øke den rettslige forutsigbarheten, samt unionsmarkedets konkurranseevne og vekst, for å bidra til å styrke det globale samarbeidet om standardisering og ta hensyn til eksisterende internasjonale standarder på KI-området som er i samsvar med Unionens verdier, grunnleggende rettigheter og interesser, og for å styrke flerpartsforvaltning som sikrer en balansert representasjon av interesser og effektiv deltakelse av alle relevante berørte parter 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 fastsatt i avsnitt 2 i dette kapitlet eller, dersom det er relevant, for forpliktelsene fastsatt i avsnitt 2 og 3 i kapittel V, dersom følgende vilkår er oppfylt:

a) Kommisjonen har i samsvar med artikkel 10 nr. 1 i forordning (EU) nr. 1025/2012 anmodet én eller flere europeiske standardiseringsorganisasjoner om å utarbeide utkast til harmoniserte standarder for kravene i avsnitt 2 i dette kapitlet, eller, dersom det er relevant, for forpliktelsene i avsnitt 2 og 3 i kapittel V, og

i) anmodningen er ikke blitt godtatt av noen av de europeiske standardiseringsorganisasjonene, eller

- ii) de harmoniserte standardene som denne anmodningen gjelder, er ikke utarbeidet innen fristen fastsatt i samsvar med artikkel 10 nr. 1 i forordning (EU) nr. 1025/2012, eller
 - iii) de relevante harmoniserte standardene tar ikke i tilstrekkelig grad hensyn til spørsmål om grunnleggende rettigheter, eller
 - iv) de harmoniserte standardene er ikke i samsvar med anmodningen, og
- b) det er ikke offentliggjort noen henvisninger til harmoniserte standarder som omfatter kravene nevnt i avsnitt 2 i dette kapitlet eller, dersom det er relevant, forpliktelsene nevnt i avsnitt 2 og 3 i kapittel V, i *Den europeiske unions tidende* i samsvar med forordning (EU) nr. 1025/2012, og det forventes ikke å bli offentliggjort noen slike henvisninger innen rimelig tid.

Når Kommisjonen utarbeider de felles spesifikasjonene, skal den rådspørre det rådgivende forumet nevnt i artikkel 67.

Gjennomføringsrettsaktene nevnt i første ledd i dette nummeret skal vedtas etter undersøkelsesprosedyren 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 at vilkårene fastsatt i nr. 1 i denne artikkelen er oppfylt.

3. KI-systemer med høy risiko eller KI-modeller for allmenne formål som er i samsvar med de felles spesifikasjonene nevnt i nr. 1, eller deler av disse spesifikasjonene, skal anses for å være i samsvar med kravene i avsnitt 2 i dette kapitlet eller, dersom det er relevant, for å oppfylle forpliktelsene i avsnitt 2 og 3 i kapittel V, i den grad disse felles spesifikasjonene omfatter nevnte krav eller forpliktelser.

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

5. Dersom leverandører av KI-systemer med høy risiko eller KI-modeller for allmenne formål ikke oppfyller de felles spesifikasjonene nevnt i nr. 1, skal de behørig dokumentere at de har tatt i bruk tekniske løsninger som oppfyller kravene i avsnitt 2 i dette kapitlet, eller, dersom det er relevant, oppfyller forpliktelsene i avsnitt 2 og 3 i kapittel V, til en grad som minst tilsvarende nevnte felles spesifikasjoner.

6. Dersom en medlemsstat anser at en felles spesifikasjon ikke fullt ut oppfyller kravene i avsnitt 2 eller, dersom det er relevant, overholder forpliktelsene i avsnitt 2 og 3 i kapittel V, skal medlemsstaten underrette Kommisjonen om dette med en detaljert forklaring. Kommisjonen skal vurdere disse opplysningene og eventuelt endre gjennomføringsrettsakten som fastsetter den aktuelle felles spesifikasjonen.

Artikkel 42

Formodning om samsvar med visse krav

1. KI-systemer med høy risiko som er trent og testet på data som avspeiler de særskilte geografiske, atferdsmessige, kontekstuelle eller funksjonelle omgivelsene der de er ment å brukes, skal formodes å være i samsvar med de relevante kravene i artikkel 10 nr. 4.

2. KI-systemer med høy risiko som er sertifisert eller som det er utstedt en samsvarserklæring for i henhold til en cybersikkerhetsordning i samsvar med forordning (EU) 2019/881, og som det er offentliggjort henvisninger til i *Den europeiske unions tidende*, skal formodes å oppfylle cybersikkerhetskravene i artikkel 15 i denne forordningen i det omfanget cybersikkerhetssertifikatet eller samsvarserklæringen eller deler av disse dekker disse cybersikkerhetskravene.

*Artikkel 43***Samsvarsvurdering**

1. For KI-systemer med høy risiko oppført i vedlegg III nr. 1 der, når leverandøren for å dokumentere at et KI-system med høy risiko oppfyller kravene i avsnitt 2, har anvendt harmoniserte standarder som omhandlet i artikkel 40 eller, dersom det er relevant, felles spesifikasjoner som omhandlet i artikkel 41, skal leverandøren velge en av de følgende samsvarsvurderingsprosedyrene på grunnlag av

- a) internkontrollen som er omhandlet i vedlegg VI, eller
- b) vurderingen av kvalitetsstyringssystemet og vurderingen av den tekniske dokumentasjonen med medvirkning fra et meldt organ som er omhandlet i vedlegg VII.

Når leverandøren skal dokumentere at et KI-system med høy risiko oppfyller kravene i avsnitt 2, skal den følge samsvarsvurderingsprosedyren i vedlegg VII dersom

- a) harmoniserte standarder som omhandlet i artikkel 40 ikke finnes, og felles spesifikasjoner som omhandlet i artikkel 41 ikke er tilgjengelige,
- b) leverandøren ikke har anvendt, eller har anvendt bare en del av, den harmoniserte standarden,
- c) de felles spesifikasjonene nevnt i bokstav a) finnes, men leverandøren ikke har anvendt dem,
- d) en eller flere av de harmoniserte standardene det vises til i bokstav a), er offentliggjort med en begrensning og bare for den delen av standarden som er begrenset.

I forbindelse med samsvarsvurderingsprosedyren omhandlet i vedlegg VII kan leverandøren velge hvilket som helst av de meldte organene. Dersom KI-systemet med høy risiko er ment å tas i bruk av rettshåndhevende myndigheter, innvandrings- eller asylmyndigheter eller Unionens institusjoner, organer, kontorer eller byråer, skal imidlertid markedstilsynsmyndigheten omhandlet i artikkel 74 nr. 8 eller 9, alt etter hva som er relevant, fungere som meldt organ.

2. For KI-systemer med høy risiko som omhandlet i nr. 2–8 i vedlegg III skal leverandørene følge samsvarsvurderingsprosedyren basert på internkontroll som er omhandlet i vedlegg VI, som ikke har krav om medvirkning fra et meldt organ.

3. For KI-systemer med høy risiko som omfattes av EU-harmoniseringsregelverket angitt i avsnitt A i vedlegg I, skal leverandøren følge den relevante samsvarsvurderingsprosedyren som kreves i disse rettsaktene. Kravene i avsnitt 2 i dette kapitlet får anvendelse på disse KI-systemene med høy risiko og skal inngå i denne vurderingen. Nr. 4.3, 4.4, 4.5 og nr. 4.6 femte ledd i vedlegg VII får også anvendelse.

Ved denne vurderingen skal meldte organer som er meldt i henhold til disse rettsaktene, ha rett til å kontrollere at KI-systemene med høy risiko oppfyller kravene i avsnitt 2, forutsatt at disse meldte organenes oppfyllelse av kravene fastsatt i artikkel 31 nr. 4, 5, 10 og 11 er vurdert i forbindelse med meldingsprosedyren i disse rettsaktene.

Dersom en rettsakt oppført i avsnitt A i vedlegg I gjør det mulig for produkttilvirkeren å velge å ikke delta i en tredjeparts samsvarsvurdering, kan denne tilvirkeren, dersom den har anvendt alle harmoniserte standarder som omfatter alle relevante krav, bare bruke dette alternativet dersom den også har anvendt harmoniserte standarder eller, dersom det er relevant, felles spesifikasjoner omhandlet i artikkel 41, som omfatter alle kravene i avsnitt 2 i dette kapitlet.

4. KI-systemer med høy risiko som allerede har vært gjenstand for en samsvarsvurderingsprosedyre, skal gjennomgå en ny samsvarsvurderingsprosedyre dersom det er gjort en vesentlig endring, uavhengig av om det endrede systemet skal distribueres videre eller fortsatt skal brukes av den aktuelle idriftsetteren.

For KI-systemer med høy risiko som fortsetter å lære etter at de er brakt i omsetning eller tatt i bruk, skal endringer i KI-systemet og dets ytelse som på forhånd er blitt bestemt av leverandøren på tidspunktet for den første samsvarsvurderingen, og som inngår i informasjonen i den tekniske dokumentasjonen omhandlet 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 artikkelen for det formålet at KI-systemer med høy risiko som omhandlet i nr. 2–8 i vedlegg III skal underkastes samsvarsvurderingsprosedyren omhandlet i vedlegg VII eller deler av den. Kommisjonen skal vedta slike delegerte rettsakter under hensyn til hvor effektiv samsvarsvurderingsprosedyren basert på internkontroll omhandlet i vedlegg VI er når det gjelder å forebygge eller minimere risikoen for helse og sikkerhet og for vernet av de grunnleggende rettighetene som slike systemer medfører, samt til om de meldte organene har tilstrekkelig kapasitet og tilstrekkelige ressurser.

Artikkel 44

Sertifikater

1. Sertifikater utstedt av meldte organer i samsvar med vedlegg VII skal utarbeides på et språk som lett kan forstås av de relevante myndighetene i medlemsstaten der det meldte organet er etablert.
2. Sertifikatene skal være gyldige i den perioden som er angitt i dem, som skal være høyst fem år for KI-systemer omfattet av vedlegg I og høyst fire år for KI-systemer omfattet av vedlegg III. Etter anmodning fra leverandøren kan gyldigheten av et sertifikat forlenges med ytterligere perioder, hver på høyst fem år for KI-systemer omfattet av vedlegg I og høyst fire år for KI-systemer omfattet av vedlegg III, på grunnlag av en ny vurdering i samsvar med de gjeldende samsvarsvurderingsprosedyrene. Et eventuelt tillegg til et sertifikat skal forbli gyldig, forutsatt at sertifikatet det er et tillegg til, er gyldig.
3. Dersom et meldt organ fastslår at et KI-system ikke lenger oppfyller kravene i avsnitt 2, skal det, idet det tar hensyn til forholdsmessighetsprinsippet, suspendere eller trekke tilbake det utstedte sertifikatet eller legge begrensninger på det, med mindre oppfyllelse av disse kravene sikres ved egnede korrigerende tiltak som treffes av leverandøren av systemet innen en egnet frist fastsatt av det meldte organet. Det meldte organet skal begrunne sin beslutning.

Det skal være adgang til å klage på det meldte organets beslutninger, herunder på utstedte samsvarssertifikater.

Artikkel 45

Meldte organers opplysningsplikt

1. Meldte organer skal underrette meldermyndigheten om følgende:
 - a) Alle EU-sertifikater for vurdering av teknisk dokumentasjon, alle tillegg til disse sertifikatene og alle godkjenninger av kvalitetsstyringssystemet utstedt i samsvar med kravene i vedlegg VII.
 - b) Alle tilfeller av avslag, begrensning, suspensjon eller tilbaketrekking av et EU-sertifikat for vurdering av teknisk dokumentasjon eller en godkjenning av et kvalitetsstyringssystem utstedt i samsvar med kravene i vedlegg VII.
 - c) Alle omstendigheter som påvirker omfanget av eller vilkårene for meldingen.
 - d) Alle anmodninger om informasjon om samsvarsvurderingsaktiviteter som de har mottatt fra markedstilsynsmyndighetene.
 - e) På anmodning, samsvarsvurderingsaktiviteter som er utført innenfor rammen av meldingen, og enhver annen aktivitet som er utført, herunder aktiviteter og underleveranser på tvers av landegrensene.
2. Hvert meldt organ skal underrette de andre meldte organene om
 - a) godkjenninger av kvalitetsstyringssystemer som det har nektet, suspendert eller trukket tilbake, og, på anmodning, godkjenninger av kvalitetsstyringssystemer som det har utstedt,
 - b) EU-sertifikater for vurdering av teknisk dokumentasjon eller eventuelle tillegg til disse som det har avslått, trukket tilbake, suspendert eller på annen måte begrenset, og, på anmodning, sertifikater og/eller tillegg til disse som det har utstedt.

3. Hvert meldt organ skal gi de andre meldte organene som utfører tilsvarende samsvarsvurderingsaktiviteter som dekker de samme typene av KI-systemer, relevant informasjon om spørsmål knyttet til negative og, på anmodning, positive resultater av samsvarsvurderinger.
4. Meldte organer skal sikre fortrolighet om den informasjonen de kommer i besittelse av, i samsvar med artikkel 78.

Artikkel 46

Unntak fra samsvarsvurderingsprosedyren

1. Som unntak fra artikkel 43 og på behørig begrunnet anmodning kan en markedstilsynsmyndighet tillate at bestemte KI-systemer med høy risiko bringes i omsetning eller tas i bruk på territoriet til den medlemsstaten det gjelder, av ekstraordinære grunner knyttet til offentlig sikkerhet eller for å verne menneskers liv og helse, miljøet eller viktig industri og infrastruktur. Denne tillatelsen skal gjelde i en begrenset periode mens de nødvendige samsvarsvurderingsprosedyrene gjennomføres, idet det tas hensyn til de ekstraordinære grunnene til at unntaket gis. Nevnte prosedyrer skal fullføres uten unødig opphold.
2. I en behørig begrunnet hastesituasjon der det foreligger ekstraordinære grunner knyttet til offentlig sikkerhet eller en spesifikk, vesentlig og overhengende trussel mot mennesker liv eller fysiske sikkerhet, kan de rettshåndhevende myndighetene eller myndighetene for sivil beredskap ta i bruk et bestemt KI-system med høy risiko uten tillatelsen nevnt i nr. 1, forutsatt at det uten ugrunnet opphold søkes slik tillatelse under eller etter bruken. Dersom tillatelsen nevnt i nr. 1 nektes, skal bruken av KI-systemet med høy risiko umiddelbart stoppes, og alle resultater og utdata fra slik bruk skal umiddelbart kasseres.
3. Tillatelsen nevnt i nr. 1 skal utstedes bare dersom markedstilsynsmyndigheten konkluderer med at KI-systemet med høy risiko oppfyller kravene i avsnitt 2. Markedstilsynsmyndigheten skal underrette Kommisjonen og de andre medlemsstatene om enhver tillatelse utstedt i henhold til nr. 1 og 2. Denne forpliktelsen omfatter ikke sensitive operasjonelle data om rettshåndhevende myndigheters virksomhet.
4. Dersom verken en medlemsstat eller Kommisjonen har reist innvendinger mot en tillatelse utstedt av en markedstilsynsmyndighet i en medlemsstat innen 15 kalenderdager etter at underretningen nevnt i nr. 3 er mottatt, skal tillatelsen anses for å være berettiget.
5. Dersom en medlemsstat innen 15 kalenderdager etter å ha mottatt underretningen nevnt i nr. 3 reiser innvendinger mot en tillatelse utstedt av en markedstilsynsmyndighet i en annen medlemsstat, eller dersom Kommisjonen anser at tillatelsen strider mot unionsretten eller at medlemsstatenes konklusjon om systemets oppfyllelse av kravene som nevnt i nr. 3 er ugrunnet, skal Kommisjonen umiddelbart innlede samråd med den relevante medlemsstaten. De berørte operatørene skal rådspørres og ha mulighet til å legge fram sine synspunkter. På grunnlag av dette skal Kommisjonen beslutte om tillatelsen er berettiget. Kommisjonen skal rette sin beslutning til medlemsstaten det gjelder, og til de relevante operatørene.
6. Dersom Kommisjonen anser at tillatelsen ikke er berettiget, skal markedstilsynsmyndigheten i medlemsstaten det gjelder, trekke den tilbake.
7. Når det gjelder KI-systemer med høy risiko som er knyttet til produkter omfattet av EU-harmoniseringsregelverket oppført i avsnitt A i vedlegg I, er det bare de unntakene fra samsvarsvurderingen som er fastsatt i nevnte EU-harmoniseringsregelverk, som får anvendelse.

Artikkel 47

EU-samsvarserklæring

1. Leverandøren skal utarbeide en skriftlig, maskinlesbar og fysisk eller elektronisk signert EU-samsvarserklæring for hvert KI-system med høy risiko og kunne stille den til rådighet for de nasjonale myndighetene i ti år etter at systemet er brakt i omsetning. EU-samsvarserklæringen skal angi hvilket KI-system med høy risiko som den er utarbeidet for. En kopi av EU-samsvarserklæringen skal leveres til de relevante nasjonale vedkommende myndighetene på anmodning.

2. Det skal framgå av EU-samsvarserklæringen at det aktuelle KI-systemet med høy risiko oppfyller kravene fastsatt i avsnitt 2. EU-samsvarserklæringen skal inneholde opplysningene angitt i vedlegg V og oversettes til et språk som lett kan forstås av de nasjonale vedkommende myndighetene i de medlemsstatene der KI-systemet med høy risiko bringes i omsetning eller gjøres tilgjengelig.
3. Dersom KI-systemer med høy risiko omfattes av annet EU-harmoniseringsregelverk som også krever en EU-samsvarserklæring, skal det utarbeides bare én EU-samsvarserklæring for all unionsrett som får anvendelse på KI-systemer med høy risiko. Erklæringen skal inneholde all informasjon som er nødvendig for å identifisere hvilket EU-harmoniseringsregelverk erklæringen viser til.
4. Ved å utarbeide EU-samsvarserklæringen påtar leverandøren seg ansvaret for at kravene fastsatt i avsnitt 2 oppfylles. Leverandøren skal oppdatere EU-samsvarserklæringen ved behov.
5. Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 for å oppdatere innholdet i EU-samsvarserklæringen i vedlegg V med nye elementer som blir nødvendige på bakgrunn av den tekniske utviklingen.

Artikkel 48

CE-merking

1. CE-merkingen er underlagt de allmenne prinsippene i artikkel 30 i forordning (EF) nr. 765/2008.
2. For KI-systemer med høy risiko som leveres digitalt, skal det brukes en digital CE-merking bare dersom den er lett tilgjengelig via det grensesnittet som man får tilgang til systemet fra, eller via en lett tilgjengelig maskinlesbar kode eller andre elektroniske midler.
3. CE-merkingen skal påføres KI-systemer med høy risiko på en slik måte at den er synlig, lett leselig og ikke kan fjernes. Dersom KI-systemet med høy risiko er av en slik art at dette ikke er mulig eller berettiget, skal den påføres emballasjen eller følgedokumentene, alt etter hva som er hensiktsmessig.
4. Dersom det er relevant, skal CE-merkingen ledsages av identifikasjonsnummeret til det meldte organet som har ansvar for samsvarsvurderingsprosedyren fastsatt i artikkel 43. Det meldte organets identifikasjonsnummer skal påføres av organet selv eller av leverandøren eller leverandørens bemyndigede representant etter organets anvisning. Identifikasjonsnummeret skal også angis i alt salgsmateriell der det nevnes at KI-systemet med høy risiko oppfyller kravene til CE-merking.
5. Dersom utstyret omfattes av annet EU-regelverk som også inneholder bestemmelser om påføring av CE-merking, skal det framgå av CE-merkingen at KI-systemet med høy risiko også oppfyller kravene i dette andre regelverket.

Artikkel 49

Registrering

1. Før et KI-system med høy risiko oppført i vedlegg III bringes i omsetning eller tas i bruk, med unntak av KI-systemer med høy risiko som nevnt i vedlegg III nr. 2, skal leverandøren eller, dersom det er relevant, den bemyndigede representanten registrere seg og sitt system i EU-databasen omhandlet i artikkel 71.
2. Før et KI-system der leverandøren har konkludert med at systemet ikke er et KI-system med høy risiko i samsvar med artikkel 6 nr. 3, bringes i omsetning eller tas i bruk, skal denne leverandøren eller, dersom det er relevant, den bemyndigede representanten registrere seg og det systemet i EU-databasen omhandlet i artikkel 71.
3. Før de tar i bruk eller bruker et KI-system med høy risiko oppført i vedlegg III, med unntak av KI-systemer med høy risiko som nevnt i vedlegg III nr. 2, skal idriftsettere som er offentlige myndigheter eller Unionens institusjoner, organer, kontorer eller byråer, eller personer som handler på disses vegne, registrere seg, velge systemet og registrere bruken av det i EU-databasen omhandlet i artikkel 71.

4. For KI-systemer med høy risiko omhandlet i vedlegg III nr. 1, 6 og 7, på områdene rettshåndhevelse og migrasjons-, asyl- og grensekontrollforvaltning, skal registreringen omhandlet i nr. 1, 2 og 3 i denne artikkelen skje i en sikker, ikke-offentlig del av EU-databasen omhandlet i artikkel 71 og skal bare omfatte opplysningene angitt i følgende bestemmelser, alt etter hva som er relevant:

- a) Avsnitt A nr. 1–10 i vedlegg VIII, med unntak av nr. 6, 8 og 9.
- b) Avsnitt B nr. 1–5 og nr. 8 og 9 i vedlegg VIII.
- c) Avsnitt C nr. 1–3 i vedlegg VIII.
- d) Nr. 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 angitt i første ledd i dette nummeret.

5. KI-systemer med høy risiko nevnt i nr. 2 i vedlegg III skal registreres på nasjonalt plan.

KAPITTEL IV

ÅPENHETSFORPLIKTELSE FOR LEVERANDØRER OG IDRIFTSETTERE AV VISSE KI-SYSTEMER

Artikkel 50

Åpenhetsforpliktelser for leverandører og idriftsettere av visse KI-systemer

1. Leverandørene 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 fysiske personene varsles om at de samhandler med et KI-system, med mindre dette er åpenbart for en fysisk person som er rimelig velinformert, observant og aktsom, tatt i betraktning omstendighetene og brukskonteksten. Denne forpliktelsen skal ikke gjelde for KI-systemer som er godkjent ved lov til å brukes for å avsløre, forebygge, etterforske eller straffeforfølge straffbare forhold, forutsatt at det gis tilstrekkelige garantier for vern av fysiske personers grunnleggende rettigheter og friheter, med mindre disse systemene er gjort tilgjengelige for offentligheten for å gjøre det mulig å melde fra om straffbare forhold.

2. Leverandører av KI-systemer, herunder KI-systemer for allmenne formål, som genererer syntetisk lyd-, bilde-, video- eller tekstinhold, skal sikre at utdataene fra KI-systemet er merket i et maskinlesbart format og identifiserbare som kunstig generert eller manipulert. Leverandørene skal sikre at deres tekniske løsninger er effektive, samvirkende, robuste og pålitelige så langt dette er teknisk mulig, idet det tas hensyn til særtrekkene og begrensningene ved ulike typer innhold, gjennomføringskostnadene og det allment anerkjente aktuelle tekniske utviklingstrinnet, som kan være gjenspeilet i relevante tekniske standarder. Denne forpliktelsen skal ikke gjelde i den grad KI-systemene utfører en hjelpefunksjon for standardredigering eller ikke i vesentlig grad endrer inndataene fra idriftsetteren eller semantikken i disse, eller dersom de er godkjent ved lov til å brukes for å avsløre, forebygge, etterforske eller straffeforfølge straffbare forhold.

3. Idriftsettere av et følelsesgjenkjenningssystem eller et biometrisk kategoriseringssystem skal underrette de fysiske personene som eksponeres for systemet, om at systemet er i drift, og skal behandle personopplysningene i samsvar med forordning (EU) 2016/679 og (EU) 2018/1725 og direktiv (EU) 2016/680. Denne forpliktelsen skal ikke gjelde for KI-systemer brukt til biometrisk kategorisering og følelsesgjenkjenning som er godkjent ved lov til å brukes for å avsløre, forebygge eller etterforske straffbare forhold, forutsatt at det gis tilstrekkelige garantier for vern av fysiske personers rettigheter og friheter, og i samsvar med unionsretten.

4. Idriftsettere av et KI-system som genererer eller manipulerer bilde-, lyd- eller videoinnhold som utgjør en dypforfalskning, skal opplyse om at innholdet er kunstig generert eller manipulert. Denne forpliktelsen skal ikke gjelde dersom bruken er godkjent ved lov for å avsløre, forebygge, etterforske eller straffeforfølge straffbare forhold. Dersom innholdet inngår i et åpenbart kunstnerisk, kreativt, satirisk, fiktivt eller tilsvarende verk eller program, er åpenhetsforpliktelsene i dette nummeret begrenset til å opplyse om at slikt generert eller manipulert innhold forekommer, på en hensiktsmessig måte som ikke hindrer at verket vises fram eller nyles.

Idriftsettere av et KI-system som genererer eller manipulerer tekst som offentliggjøres for å informere allmennheten om saker av allmenn interesse, skal opplyse om at teksten er kunstig generert eller manipulert. Denne forpliktelsen skal ikke gjelde dersom bruken er godkjent ved lov for å avsløre, forebygge, etterforske eller straffeforfølge straffbare forhold, eller dersom det KI-genererte innholdet er gjennomgått av mennesker eller har vært gjenstand for redaksjonell kontroll, og en fysisk eller juridisk person har redaksjonelt ansvar for offentliggjøringen av innholdet.

5. Informasjonen nevnt i nr. 1–4 skal meddeles de berørte fysiske personene på en klar og tydelig måte senest på tidspunktet for den første samhandlingen eller eksponeringen. Informasjonen skal være i samsvar med de gjeldende tilgjengelighetskravene.

6. Nr. 1–4 skal ikke påvirke kravene og forpliktelsene fastsatt i kapittel III og skal ikke berøre andre åpenhetsforpliktelser fastsatt i unionsretten eller nasjonal rett for idriftsettere av KI-systemer.

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

KAPITTEL V

KI-MODELLER FOR ALLMENNE FORMÅL

AVSNITT 1

Klassifiseringsregler

Artikkel 51

Klassifisering av KI-modeller for allmenne formål som KI-modeller for allmenne formål med systemrisiko

1. En KI-modell for allmenne formål skal klassifiseres som en KI-modell for allmenne formål med systemrisiko dersom den oppfyller et av følgende vilkår:
 - a) Den har kapabiliteter med høy påvirkningsgrad, vurdert på grunnlag av egnede tekniske verktøy og metoder, herunder indikatorer og referanseverdier.
 - b) På grunnlag av en beslutning som Kommisjonen treffer på eget initiativ eller etter et kvalifisert varsel fra vitenskapspanelet, har den kapabiliteter eller en innvirkning som tilsvarer det som er angitt i bokstav a), i betraktning av kriteriene angitt i vedlegg XIII.
2. En KI-modell for allmenne formål skal antas å ha kapabiliteter med høy påvirkningsgrad i henhold til nr. 1 bokstav a) når den samlede regnekraften som brukes til treningen av den, målt i antall flyttallsoperasjoner, er større enn 10^{25} .
3. Kommisjonen skal vedta delegerte rettsakter i samsvar med artikkel 97 for å endre tersklene som er angitt i nr. 1 og 2 i denne artikkelen, samt for å supplere referanseverdier og indikatorer i lys av den teknologiske utviklingen, for eksempel algoritmiske forbedringer eller mer effektiv maskinvare, når det er nødvendig for at disse tersklene skal gjenspeile det aktuelle tekniske utviklingstrinnet.

Artikkel 52

Prosedyre

1. Dersom en KI-modell for allmenne formål oppfyller vilkåret nevnt i artikkel 51 nr. 1 bokstav a), skal den relevante leverandøren underrette Kommisjonen om dette uten ugrunnet opphold og under alle omstendigheter innen to uker etter at dette kravet er oppfylt eller det blir kjent at det vil bli oppfylt. Underretningen skal omfatte de opplysningene som er nødvendige for å vise at det relevante kravet er oppfylt. Dersom Kommisjonen får kjennskap til en KI-modell for allmenne formål som innebærer systemrisiko som den ikke er blitt underrettet om, kan den beslutte å utpeke den som en modell med systemrisiko.
2. Leverandøren av en KI-modell for allmenne formål som oppfyller vilkåret nevnt i artikkel 51 nr. 1 bokstav a), kan sammen med underretningen framlegge tilstrekkelig underbygde argumenter for å vise at KI-modellen for allmenne formål unntaksvis, selv om den oppfyller dette kravet, på grunn av sine særlige egenskaper ikke innebærer systemrisiko og derfor ikke bør klassifiseres som en KI-modell for allmenne formål med systemrisiko.

3. Dersom Kommisjonen konkluderer med at argumentene framlagt i henhold til nr. 2 ikke er tilstrekkelig underbygd, og at den relevante leverandøren ikke har kunnet vise at KI-modellen for allmenne formål på grunn av sine særlige egenskaper ikke innebærer systemrisiko, skal den avvise disse argumentene, og modellen skal anses for å være en KI-modell for allmenne formål med systemrisiko.

4. Kommisjonen kan på eget initiativ eller etter et kvalifisert varsel fra vitenskapspanelet i henhold til artikkel 90 nr. 1 bokstav a) utpeke en KI-modell for allmenne formål som en modell som innebærer systemrisiko, på grunnlag av kriteriene angitt i vedlegg XIII.

Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 for å endre vedlegg VIII ved å spesifisere og oppdatere kriteriene angitt i det vedlegget.

5. Etter begrunnet anmodning fra en leverandør av en modell som er utpekt som en KI-modell for allmenne formål med systemrisiko i samsvar med nr. 4, skal Kommisjonen ta hensyn til anmodningen og kan beslutte å foreta en ny vurdering for å fastslå om KI-modellen for allmenne formål fortsatt kan anses å innebære systemrisiko på grunnlag av kriteriene angitt i vedlegg XIII. En slik anmodning skal omfatte objektive, detaljerte og nye grunner som har framkommet etter utpekingsbeslutningen. Leverandører kan anmode om en ny vurdering tidligst seks måneder etter utpekingsbeslutningen. Dersom Kommisjonen etter sin nye vurdering beslutter å opprettholde utpekingen av modellen som en KI-modell for allmenne formål med systemrisiko, kan leverandørene anmode om en ny vurdering igjen tidligst seks måneder etter denne beslutningen.

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

AVSNITT 2

Forpliktelser for leverandører av KI-modeller for allmenne formål

Artikkel 53

Forpliktelser for leverandører av KI-modeller for allmenne formål

1. Leverandører av KI-modeller for allmenne formål skal
 - a) utarbeide og holde oppdatert den tekniske dokumentasjonen om modellen, herunder trenings- og testprosessen og resultatene av evalueringen, som minst skal inneholde opplysningene angitt i vedlegg XI, for på anmodning å gi den til KI-kontoret og de nasjonale vedkommende myndighetene,
 - b) utarbeide, holde oppdatert og gjøre tilgjengelig informasjon og dokumentasjon for leverandører av KI-systemer som har til hensikt å integrere KI-modellen for allmenne formål i sine KI-systemer. Uten at det berører nødvendigheten av å overholde og beskytte immaterielle rettigheter, fortrolig forretningsinformasjon og forretningshemmeligheter i samsvar med unionsretten og nasjonal rett, skal informasjonen og dokumentasjonen
 - i) gjøre det mulig for leverandører av KI-systemer å ha en god forståelse av kapabilitetene og begrensningene i KI-modellen for allmenne formål og å oppfylle sine forpliktelser i henhold til denne forordningen, og
 - ii) minst inneholde opplysningene angitt i vedlegg XII,
 - c) innføre en framgangsmåte for å overholde unionsretten om opphavsrett og nærstående rettigheter, og særlig for å identifisere og etterleve, herunder ved hjelp av den nyeste teknologien, forbeholdelse av rettigheter i samsvar med artikkel 4 nr. 3 i direktiv (EU) 2019/790,
 - d) utarbeide og offentliggjøre et tilstrekkelig detaljert sammendrag av innholdet som er brukt til treningen av KI-modellen for allmenne formål, i samsvar med en mal som leveres av KI-kontoret.

2. Forpliktelsene fastsatt i nr. 1 bokstav a) og b) får ikke anvendelse på leverandører av KI-modeller som utgis under en lisens med fri og åpen kildekode som tillater tilgang til og bruk, endring og distribusjon av modellen, og hvis parametere, herunder vektene, informasjonen om modellarkitekturen og informasjonen om modellbruken, gjøres offentlig tilgjengelige. Dette unntaket skal ikke gjelde for KI-modeller for allmenne formål med systemrisiko.
3. Leverandører av KI-modeller for allmenne formål skal samarbeide med Kommisjonen og de nasjonale vedkommende myndighetene når de utøver sin kompetanse og myndighet i samsvar med denne forordningen.
4. Leverandører av KI-modeller for allmenne formål kan vise til regler for god praksis som omhandlet i artikkel 56 for å dokumentere at de overholder forpliktelsene fastsatt i nr. 1 i denne artikkelen, inntil det offentliggjøres en harmonisert standard. Overholdelse av europeiske harmoniserte standarder gir leverandørene formodning om samsvar så langt standardene omfatter nevnte forpliktelser. Leverandører av KI-modeller for allmenne formål som ikke overholder godkjente regler for god praksis eller en europeisk harmonisert standard, skal vise at de har andre egnede midler til å dokumentere overholdelse, som skal vurderes av Kommisjonen.
5. For å lette overholdelsen av vedlegg XI, særlig nr. 2 bokstav d) og e), gis Kommisjonen myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 for å spesifisere måle- og beregningsmetoder med sikte på å oppnå sammenlignbar og verifiserbar dokumentasjon.
6. Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 97 nr. 2 for å endre vedlegg XI og XII i lys av den tekniske utviklingen.
7. All informasjon eller dokumentasjon som innhentes i samsvar med denne artikkelen, herunder forretningshemmeligheter, skal behandles i samsvar med fortrolighetsforpliktelsene i artikkel 78.

Artikkel 54

Bemyndigede representanter for leverandører av KI-modeller for allmenne formål

1. Før de bringer KI-modeller for allmenne formål i omsetning, skal leverandører som er etablert i tredjeland, ved skriftlig fullmakt utpeke en bemyndiget representant som er etablert i Unionen.
2. Leverandøren skal sette sin bemyndigede representant i stand til å utføre de oppgavene som er angitt i fullmakten fra leverandøren.
3. Den bemyndigede representanten skal utføre de oppgavene som er angitt i fullmakten fra leverandøren. Den skal på anmodning framlegge en kopi av fullmakten for KI-kontoret på et av de offisielle språkene til Unionens institusjoner. For denne forordningens formål skal fullmakten gi den bemyndigede representanten myndighet til å utføre følgende oppgaver:
 - a) Kontrollere at den tekniske dokumentasjonen angitt i vedlegg XI er blitt utarbeidet, og at leverandøren har oppfylt alle forpliktelsene nevnt i artikkel 53 og eventuelt artikkel 55.
 - b) Oppbevare en kopi av den tekniske dokumentasjonen angitt i vedlegg XI og kunne stille den til rådighet for KI-kontoret og nasjonale vedkommende myndigheter i et tidsrom på ti år etter at KI-modellen for allmenne formål er brakt i omsetning, samt kontaktopplysningene til den leverandøren som utnevnte den bemyndigede representanten.
 - c) På begrunnet anmodning gi KI-kontoret alle opplysninger og all dokumentasjon, herunder den som er nevnt i bokstav b), som er nødvendig for å vise at forpliktelsene i dette kapittelet er oppfylt.
 - d) På begrunnet anmodning samarbeide med KI-kontoret og vedkommende myndigheter om alle tiltak de treffer i forbindelse med KI-modellen for allmenne formål, også når modellen er integrert i KI-systemer som bringes i omsetning eller tas i bruk i Unionen.
4. Fullmakten skal gi den bemyndigede representanten rett til, i tillegg til eller i stedet for leverandøren, å motta henvendelser fra KI-kontoret eller vedkommende myndigheter i alle spørsmål som gjelder overholdelse av denne forordningen.

5. Den bemyndigede representanten skal si opp fullmakten dersom denne anser eller har grunn til å anta at leverandøren opptrer i strid med sine forpliktelser etter denne forordningen. I slike tilfeller skal den også umiddelbart underrette KI-kontoret om at fullmakten er oppsagt, og om årsakene til dette.

6. Forpliktelsene fastsatt i denne artikkelen får ikke anvendelse på leverandører av KI-modeller for allmenne formål som utgis under en lisens med fri og åpen kildekode som tillater tilgang til og bruk, endring og distribusjon av modellen, og hvis parametere, herunder vektene, informasjonen om modellarkitekturen og informasjonen om modellbruken, gjøres offentlig tilgjengelige, med mindre KI-modellene for allmenne formål innebærer systemrisiko.

AVSNITT 3

Forpliktelser for leverandører av KI-modeller for allmenne formål med systemrisiko

Artikkel 55

Forpliktelser for leverandører av KI-modeller for allmenne formål med systemrisiko

1. I tillegg til å oppfylle forpliktelsene i artikkel 53 og 54 skal leverandører av KI-modeller for allmenne formål med systemrisiko
 - a) utføre modellevaluering i samsvar med standardiserte protokoller og verktøy som gjenspeiler det aktuelle tekniske utviklingstrinnet, herunder gjennomføre og dokumentere testing av modellen for ondsinnet bruk med sikte på å avdekke og begrense systemrisiko,
 - b) vurdere og redusere mulig systemrisiko på unionsplan, herunder kildene til dem, som kan skyldes at KI-modeller for allmenne formål med systemrisiko utvikles, bringes i omsetning eller brukes,
 - c) holde oversikt over, dokumentere og uten unødig opphold rapportere til KI-kontoret og, når det er hensiktsmessig, nasjonale vedkommende myndigheter relevante opplysninger om alvorlige hendelser og mulige korrigerende tiltak for å håndtere dem,
 - d) sikre tilstrekkelig vern av cybersikkerheten for KI-modellen for allmenne formål med systemrisiko og av modellens fysiske infrastruktur.
2. Leverandører av KI-modeller for allmenne formål med systemrisiko kan vise til regler for god praksis som omhandlet i artikkel 56 for å dokumentere at de overholder forpliktelsene fastsatt i nr. 1 i denne artikkelen, inntil det offentliggjøres en harmonisert standard. Overholdelse av europeiske harmoniserte standarder gir leverandørene formodning om samsvar så langt standardene omfatter nevnte forpliktelser. Leverandører av KI-modeller for allmenne formål med systemrisiko som ikke overholder godkjente regler for god praksis eller en europeisk harmonisert standard, skal vise at de har andre egnede midler til å dokumentere overholdelse, som skal vurderes av Kommisjonen.
3. All informasjon eller dokumentasjon som innhentes i samsvar med denne artikkelen, herunder forretningshemmeligheter, skal behandles i samsvar med fortrolighetsforpliktelsene i artikkel 78.

AVSNITT 4

Regler for god praksis

Artikkel 56

Regler for god praksis

1. KI-kontoret skal oppmuntre til og lette utarbeiding av regler for god praksis på unionsplan for å bidra til riktig anvendelse av denne forordningen, idet det tas hensyn til internasjonale tilnærminger.
2. KI-kontoret og KI-rådet skal ha som mål å sikre at reglene for god praksis minst omfatter forpliktelsene fastsatt i artikkel 53 og 55, herunder

- a) midlene til å sikre at opplysningene nevnt i artikkel 53 nr. 1 bokstav a) og b) holdes oppdatert i lys av markedsutviklingen og den teknologiske utviklingen,
- b) tilstrekkelig detaljnivå i sammendraget av innholdet som er brukt til treningen,
- c) identifikasjon av typen og arten av systemrisikoen på unionsplan, herunder kildene til den når det er hensiktsmessig,
- d) tiltakene, prosedyrene og metodene for å vurdere og håndtere systemrisikoen på unionsplan, herunder dokumentere den, som skal stå i forhold til risikoen, ta hensyn til hvor alvorlig og sannsynlig den er, og de særlige utfordringene ved å takle slik risiko på grunnlag av de mulige måtene den kan oppstå og materialisere seg på langs KI-verdikjeden.

3. KI-kontoret kan invitere alle leverandører av KI-modeller for allmenne formål og relevante nasjonale vedkommende myndigheter til å delta i utarbeidingen av reglene for god praksis. Sivilsamfunnsorganisasjoner, næringslivet, academia og andre relevante berørte parter, for eksempel nedstrømsleverandører og uavhengige eksperter, kan støtte prosessen.

4. KI-kontoret og KI-rådet skal ha som mål å sikre at reglene for god praksis klart angir de særlige målene med dem, og at de inneholder forpliktelser eller tiltak, herunder resultatnøkkeltall, når 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 unionsplan.

5. KI-kontoret skal ha som mål å sikre at deltakerne i reglene for god praksis regelmessig rapporterer til KI-kontoret om gjennomføringen av forpliktelsene samt om de tiltakene som er truffet, og resultatene av dem, også eventuelt målt mot resultatnøkkeltallene. Resultatnøkkeltall og rapporteringsforpliktelser skal gjenspeile forskjellene i størrelse og kapasitet mellom de ulike deltakerne.

6. KI-kontoret og KI-rådet skal overvåke og evaluere deltakernes oppnåelse av målene med reglene for god praksis og deres bidrag til korrekt anvendelse av denne forordningen. KI-kontoret og KI-rådet skal vurdere om reglene for god praksis omfatter forpliktelsene fastsatt i artikkel 53 og 55, og skal regelmessig kontrollere og evaluere oppnåelsen av målene. De skal offentliggjøre sin vurdering av egnetheten til reglene for god praksis.

Kommisjonen kan ved en gjennomføringsrettsakt godkjenne et sett med regler for god praksis og gi det allmenn gyldighet i Unionen. Denne gjennomføringsrettsakten skal vedtas i samsvar med undersøkelsesprosedyren nevnt i artikkel 98 nr. 2.

7. KI-kontoret kan oppfordre alle leverandører av KI-modeller for allmenne formål til å overholde reglene for god praksis. For leverandører av KI-modeller for allmenne formål som ikke innebærer systemrisiko, kan denne overholdelsen begrenses til forpliktelsene fastsatt i artikkel 53, med mindre leverandørene uttrykkelig oppgir at de ønsker å slutte seg til hele regelsettet.

8. KI-kontoret skal, dersom det er relevant, også oppmuntre til og legge til rette for at reglene for god praksis gjennomgås og tilpasses, særlig i lys av nye standarder. KI-kontoret skal bistå ved vurderingen av tilgjengelige standarder.

9. Regler for god praksis skal være klare senest 2. mai 2025. KI-kontoret skal treffe de nødvendige tiltakene, herunder oppfordre leverandører i samsvar med nr. 7.

Dersom reglene for god praksis ikke kan ferdigstilles innen 2. august 2025, eller dersom KI-kontoret etter sin vurdering i henhold til nr. 6 i denne artikkelen finner at de ikke er egnet, kan Kommisjonen ved hjelp av gjennomføringsrettsakter fastsette felles regler for gjennomføring av forpliktelsene fastsatt i artikkel 53 og 55, herunder aspektene omhandlet i nr. 2 i denne artikkelen. Disse gjennomføringsrettsaktene skal vedtas i samsvar med undersøkelsesprosedyren nevnt i artikkel 98 nr. 2.

KAPITTEL VI

TILTAK TIL STØTTE FOR INNOVASJON

Artikkel 57

Regulatoriske sandkasser for KI

1. Medlemsstatene skal sikre at deres vedkommende myndigheter oppretter minst én regulatorisk sandkasse for KI på nasjonalt plan, som skal være i drift innen 2. august 2026. Denne sandkassen kan også opprettes sammen med de vedkommende myndighetene i andre medlemsstater. Kommisjonen kan yte teknisk støtte, råd og verktøy for opprettelse og drift av regulatoriske sandkasser for KI.

Forpliktelsen i henhold til første ledd kan også oppfylles ved å delta i en eksisterende sandkasse, dersom denne deltakelsen gir et likeverdig nivå av nasjonal dekning for de deltakende medlemsstatene.

2. Det kan også opprettes ytterligere regulatoriske sandkasser for KI på regionalt eller lokalt plan, eller de kan opprettes sammen med vedkommende myndigheter i andre medlemsstater.

3. EUs datatilsyn kan også opprette en regulatorisk sandkasse for KI for Unionens institusjoner, organer, kontorer og byråer og kan ivareta de nasjonale vedkommende myndighetenes roller og oppgaver i samsvar med dette kapitlet.

4. Medlemsstatene skal sikre at de vedkommende myndighetene nevnt i nr. 1 og 2 setter av tilstrekkelige ressurser til å overholde denne artikkelen effektivt og til rett tid. Når det er hensiktsmessig, skal nasjonale vedkommende myndigheter samarbeide med andre relevante myndigheter, og kan gi rom for deltakelse fra andre aktører innenfor KI-økosystemet. Denne artikkelen skal ikke berøre andre regulatoriske sandkasser som er opprettet i henhold til unionsretten eller nasjonal rett. Medlemsstatene skal sikre et hensiktsmessig samarbeid mellom myndighetene som fører tilsyn med de andre sandkassene, og de nasjonale vedkommende myndighetene.

5. Regulatoriske sandkasser for KI som er opprettet i henhold til nr. 1, skal utgjøre et kontrollert miljø som fremmer innovasjon og letter utvikling, trening, testing og validering av innovative KI-systemer i en begrenset periode, før de bringes i omsetning eller tas i bruk i samsvar med en spesifikk sandkasseplan avtalt mellom leverandørene eller de prospektive leverandørene og vedkommende myndighet. Slike sandkasser kan omfatte testing under virkelige forhold under tilsyn.

6. Vedkommende myndigheter skal, dersom det er relevant, gi veiledning, tilsyn og støtte i den regulatoriske sandkassen for KI med sikte på å identifisere risiko, særlig når det gjelder grunnleggende rettigheter, helse og sikkerhet, testing, avbøtende tiltak og deres effektivitet med hensyn til forpliktelsene og kravene i denne forordningen og, dersom det er relevant, annen unionsrett og nasjonal rett som det føres tilsyn med i sandkassen.

7. Vedkommende myndigheter skal gi leverandører og prospektive leverandører som deltar i den regulatoriske sandkassen for KI, veiledning om regulatoriske forventninger og hvordan de skal oppfylle kravene og forpliktelsene fastsatt i denne forordningen.

På anmodning fra leverandøren eller den prospektive leverandøren av KI-systemet skal vedkommende myndighet framlegge skriftlig bevis på de aktivitetene som er utført med vellykket resultat i sandkassen. Vedkommende myndighet skal også framlegge en sluttrapport med nærmere opplysninger om aktivitetene som er utført i sandkassen, og resultatene og læringsutbyttet av disse. Leverandører kan bruke slik dokumentasjon til å vise at de overholder denne forordningen gjennom samsvarsvurderingsprosessen eller relevant markedstilsynsvirksomhet. I den forbindelse skal markedstilsynsmyndighetene og de meldte organene vurdere sluttrapportene og den skriftlige dokumentasjonen fra den nasjonale vedkommende myndigheten positivt, med sikte på å framskynde samsvarsvurderingsprosedyren i rimelig utstrekning.

8. Med forbehold for bestemmelsene om fortrolighet i artikkel 78 og med samtykke fra leverandøren eller den prospektive leverandøren skal Kommisjonen og KI-rådet kunne få tilgang til sluttrapportene og skal, dersom det er relevant, ta hensyn til dem når de utfører oppgavene sine i henhold til denne forordningen. Dersom både leverandøren eller den prospektive leverandøren og den nasjonale vedkommende myndigheten uttrykkelig samtykker, kan sluttrapporten gjøres offentlig tilgjengelig gjennom den felles informasjonsplattformen omhandlet i denne artikkelen.

9. Opprettelsen av regulatoriske sandkasser for KI skal ha som formål å bidra til følgende mål:

a) Forbedre den rettslige forutsigbarheten for å oppnå overholdelse av denne forordningen eller, dersom det er relevant, annen gjeldende unionsrett og nasjonal rett.

- b) Støtte deling av beste praksis gjennom samarbeid med de myndighetene som deltar i den regulatoriske sandkassen for KI.
- c) Fremme innovasjon og konkurranseevne og lette utviklingen av et KI-økosystem.
- d) Bidra til evidensbasert regulatorisk læring.
- e) Lette og framskynde tilgangen til unionsmarkedet for KI-systemer, særlig når de leveres av små og mellomstore bedrifter, herunder oppstartsbedrifter.

10. I den grad de innovative KI-systemene omfatter behandling av personopplysninger eller på annen måte faller inn under tilsynsområdet for andre nasjonale myndigheter eller vedkommende myndigheter som gir eller støtter tilgang til data, skal de nasjonale vedkommende myndighetene sikre at de nasjonale personvernmyndighetene og disse andre nasjonale eller vedkommende myndighetene er tilknyttet driften av den regulatoriske sandkassen for KI og deltar i tilsynet med disse aspektene innenfor rammen av sine respektive oppgaver og fullmakter.

11. De regulatoriske sandkassene for KI skal ikke berøre tilsynsfullmaktene eller de korrigerende fullmaktene til de vedkommende myndighetene som fører tilsyn med sandkassene, herunder på regionalt eller lokalt plan. Dersom det avdekkes betydelig risiko for helse og sikkerhet og grunnleggende rettigheter under utviklingen og testingen av slike KI-systemer, skal det treffes egnede risikoreduserende tiltak. Nasjonale vedkommende myndigheter skal ha makt til midlertidig eller permanent å avslutte testprosessen eller deltakelsen i sandkassen dersom det ikke er mulig å treffe effektive risikoreduserende tiltak, og skal informere KI-kontoret om denne beslutningen. De nasjonale vedkommende myndighetene skal utøve sin tilsynsmyndighet innenfor rammen av gjeldende rett og utøve sin skjønnsmyndighet når de gjennomfører lovbestemmelser med hensyn til et bestemt prosjekt med en regulatorisk sandkasse for KI, med det formålet å støtte innovasjon på KI-området i Unionen.

12. Leverandører og prospektive leverandører som deltar i den regulatoriske sandkassen for KI, skal forbli ansvarlige i henhold til gjeldende unionsrett og nasjonal rett om erstatningsansvar for eventuelle skader som påføres tredjeparter som følge av de forsøkene som finner sted i sandkassen. Imidlertid, forutsatt at de prospektive leverandørene overholder den spesifikke planen og vilkårene for sin deltakelse og i god tro følger retningslinjene fra den nasjonale vedkommende myndigheten, skal myndighetene ikke ilegge gebyr for overtredelser av denne forordningen. Dersom andre vedkommende myndigheter med ansvar for annen unionsrett og nasjonal rett har vært aktivt involvert i tilsynet med KI-systemet i sandkassen og gitt veiledning om overholdelse, skal det ikke ilegges overtredelsesgebyrer med hensyn til denne retten.

13. De regulatoriske sandkassene for KI skal utformes og gjennomføres på en slik måte at de, dersom det er relevant, letter samarbeid på tvers av landegrensene mellom nasjonale vedkommende myndigheter.

14. De nasjonale vedkommende myndighetene skal samordne sin virksomhet og samarbeide innenfor rammen av KI-rådet.

15. De nasjonale vedkommende myndighetene skal informere KI-kontoret og KI-rådet om opprettelsen av en sandkasse og kan be dem om støtte og veiledning. KI-kontoret skal offentliggjøre en liste over planlagte og eksisterende sandkasser og holde den oppdatert for å oppmuntre til mer samhandling i de regulatoriske sandkassene for KI og samarbeid på tvers av landegrensene.

16. De nasjonale vedkommende myndighetene skal framlegge årlige rapporter for KI-kontoret og KI-rådet fra og med ett år etter opprettelsen av den regulatoriske sandkassen for KI og deretter hvert år fram til den avsluttes, samt en sluttrapport. Disse rapportene skal gi informasjon om framdriften i og resultatene av gjennomføringen av disse sandkassene, herunder beste praksis, hendelser, erfaringer og anbefalinger om utformingen av dem og, dersom det er relevant, om anvendelsen og en mulig revisjon av denne forordningen, herunder tilhørende delegerte rettsakter og gjennomføringsrettsakter, og om anvendelsen av annen unionsrett som vedkommende myndigheter fører tilsyn med i sandkassen. De nasjonale vedkommende myndighetene skal gjøre disse årsrapportene eller sammendrag av dem tilgjengelige for offentligheten på internett. Kommisjonen skal, dersom det er relevant, ta hensyn til de årlige rapportene når den utfører sine oppgaver i henhold til denne forordningen.

17. Kommisjonen skal utarbeide et felles og særskilt grensesnitt som inneholder all relevant informasjon knyttet til regulatoriske sandkasser for KI, slik at berørte parter kan samhandle med regulatoriske sandkasser for KI og rette henvendelser til vedkommende myndigheter samt søke ikke-bindende veiledning om samsvar for innovative produkter, tjenester og forretningsmodeller som omfatter KI-teknologi, i samsvar med artikkel 62 nr. 1 bokstav c). Kommisjonen skal proaktivt samordne seg med nasjonale vedkommende myndigheter dersom det er relevant.

Artikkel 58

Nærmere ordninger for, og virkemåten til, regulatoriske sandkasser for KI

1. For å unngå fragmentering i Unionen skal Kommisjonen vedta gjennomføringsrettsakter som fastsetter de nærmere ordningene for opprettelse, utvikling, gjennomføring og drift av samt tilsyn med regulatoriske sandkasser for KI. Gjennomføringsrettsaktene skal inneholde felles prinsipper på følgende områder:

- a) Kvalifikasjons- og utvelgelseskriterier for deltakelse i den regulatoriske sandkassen for KI.
- b) Prosedyrer for bruk av, deltakelse i, tilsyn med, uttredelse fra og avslutning av den regulatoriske sandkassen for KI, herunder sandkasseplanen og sluttrapporten.
- c) Vilkårene 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 regulatoriske sandkasser for KI er åpne for alle leverandører eller prospektive leverandører av et KI-system som søker, og som oppfyller kvalifikasjons- og utvelgelseskriteriene, idet disse skal være åpne og rettferdige, og at de nasjonale vedkommende myndighetene informerer søkerne om sin beslutning innen tre måneder etter søknadsdatoen,
- b) at regulatoriske sandkasser for KI gir bred og lik tilgang og holder tritt med etterspørselen etter deltakelse; leverandører og prospektive leverandører kan også sende inn søknader i partnerskap med idriftsettere og andre relevante tredjeparter,
- c) at de nærmere bestemmelsene om og vilkårene for regulatoriske sandkasser for KI i størst mulig grad gir nasjonale vedkommende myndigheter fleksibilitet til å opprette og drive sine regulatoriske sandkasser for KI,
- d) at tilgang til de regulatoriske sandkassene for KI er gratis for små og mellomstore bedrifter, herunder oppstartsbedrifter, uten at dette berører de nasjonale vedkommende myndighetenes rett til å få dekket inn ekstraordinære kostnader på en rettferdig og forholdsmessig måte,
- e) at de ved hjelp av læringsutbyttet fra de regulatoriske sandkassene for KI gjør det lettere for leverandører og prospektive leverandører å overholde samsvarsvurderingsforpliktelsene som følger av denne forordningen, og å frivillig anvende atferdsreglene nevnt i artikkel 95,
- f) at regulatoriske sandkasser for KI letter involvering av andre relevante aktører innenfor KI-økosystemet, for eksempel meldte organer og standardiseringsorganisasjoner, små og mellomstore bedrifter, herunder oppstartsbedrifter, samt foretak, innovatører, test- og forsøksanlegg, forsknings- og forsøkslaboratorier, europeiske digitale innovasjonsnav, kompetansesentre og enkeltforskere, for å lette samarbeid med offentlig og privat sektor,
- g) at prosedyrer, prosesser og administrative krav ved søking til, utvalgelse til, deltaking i og uttredelse fra den regulatoriske sandkassen for KI er enkle, lett forståelige og klart formidlet, for å lette deltakelse fra små og mellomstore bedrifter, herunder oppstartsbedrifter, med begrenset juridisk og administrativ kapasitet, og er strømlinjeformet i hele Unionen for å unngå fragmentering, samt at deltakelse i en regulatorisk sandkasse for KI som er opprettet av en medlemsstat eller av EUs data-tilsyn, anerkjennes gjensidig og på samme måte og har samme rettsvirkning i hele Unionen,
- h) at deltakelse i den regulatoriske sandkassen for KI er begrenset til en periode som står i forhold til prosjektets kompleksitet og omfang, og som den nasjonale vedkommende myndigheten kan forlenge,
- i) at regulatoriske sandkasser for KI letter utviklingen av verktøy og infrastruktur for testing, referansemåling, vurdering og forklaring av aspekter ved KI-systemer som er relevante for regulatorisk læring, slik som riktighet, robusthet og cybersikkerhet, samt tiltak for å redusere risiko for grunnleggende rettigheter og for samfunnet som helhet.

3. Prospektive leverandører i de regulatoriske sandkassene for KI, særlig små og mellomstore bedrifter og oppstartsbedrifter, skal, når det er relevant, henvises til tjenester forut for idriftsettingen, så som veiledning om gjennomføringen av denne forordningen, og til andre verdikjende tjenester, så som hjelp med standardiseringsdokumenter og sertifisering, test- og forsøksanlegg, europeiske digitale innovasjonsnav og kompetansesentre.

4. Dersom nasjonale vedkommende myndigheter vurderer å gi tillatelse til testing under virkelige forhold som det føres tilsyn med innenfor rammen av en regulatorisk sandkasse for KI som skal opprettes i henhold til denne artikkelen, skal de uttrykkelig avtale vilkårene for denne testingen med deltakerne, og særlig de nødvendige garantiene, med sikte på å beskytte grunnleggende rettigheter, helse og sikkerhet. Når det er hensiktsmessig, skal de samarbeide med andre nasjonale vedkommende myndigheter for å sikre konsekvent praksis i hele Unionen.

Artikkel 59

Videre behandling av personopplysninger for å utvikle visse KI-systemer i allmennhetens interesse i den regulatoriske sandkassen for KI

1. I den regulatoriske sandkassen for KI kan personopplysninger som er lovlig innhentet for andre formål, utelukkende behandles for det formålet å utvikle, trene og teste visse KI-systemer i sandkassen når alle følgende vilkår er oppfylt:

- a) KI-systemene skal utvikles for å verne vesentlige allmenne interesser, av en offentlig myndighet eller en annen fysisk eller juridisk person, og på ett eller flere av følgende områder:
 - i) Offentlig sikkerhet og folkehelse, herunder påvisning, diagnostisering, forebygging og behandling av sykdommer og forbedring av helsesystemer.
 - ii) Et høyt nivå av vern og bedring av miljøkvaliteten, vern av biologiske mangfold, vern mot forurensning, tiltak for grønn omstilling samt tiltak for bekjempelse av og tilpasning til klimaendringer.
 - iii) Bærekraftig energi.
 - iv) Sikkerhet og motstandsdyktighet i transportsystemer og samferdsel, kritisk infrastruktur og transportnettverk.
 - v) Effektivitet og kvalitet i offentlig forvaltning og offentlige tjenester.
- b) Dataene som behandles, er nødvendige for å oppfylle ett eller flere av kravene omhandlet i kapittel III avsnitt 2, dersom disse kravene ikke kan oppfylles effektivt ved behandling av anonymiserte, syntetiske eller andre data som ikke er personopplysninger.
- c) Det finnes effektive overvåkingsmekanismer for å avdekke om det kan oppstå høy risiko for de registrertes rettigheter og friheter, som omhandlet i artikkel 35 i forordning (EU) 2016/679 og artikkel 39 i forordning (EU) 2018/1725, under sandkasseforsøkene, samt responsmekanismer for raskt å begrense slik risiko og om nødvendig stanse behandlingen.
- d) Eventuelle personopplysninger som skal behandles innenfor rammen av sandkassen, befinner seg i et funksjonelt atskilt, isolert og beskyttet databehandlingsmiljø under den prospektive leverandørens kontroll, og bare autoriserte personer har tilgang til disse opplysningene.
- e) Leverandører kan bare dele de opprinnelig innsamlede dataene videre i samsvar med unionsretten om vern av personopplysninger; eventuelle personopplysninger som er skapt i sandkassen, kan ikke deles utenfor sandkassen.
- f) Ingen behandling av personopplysninger innenfor rammen av sandkassen fører til tiltak eller beslutninger som berører de registrerte, og berører heller ikke anvendelsen av deres rettigheter som fastsatt i unionsretten om vern av personopplysninger.
- g) Eventuelle personopplysninger som behandles innenfor rammen av sandkassen, beskyttes ved hjelp av egnede tekniske og organisatoriske tiltak og slettes når deltakelsen i sandkassen er avsluttet, eller når lagringstiden for personopplysningene utløper.
- h) Loggene over behandlingen av personopplysninger innenfor rammen av sandkassen beholdes 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 treningen, testingen og valideringen av KI-systemet oppbevares sammen med testresultatene som en del av den tekniske dokumentasjonen omhandlet i vedlegg IV.

j) Et kort sammendrag av KI-prosjektet som er utviklet i sandkassen, målene med det og de forventede resultatene av det, offentliggjøres på vedkommende myndigheters nettsted; denne forpliktelsen omfatter ikke sensitive operasjonelle data om virksomheten til rettshåndhevende myndigheter eller grensekontroll-, innvandrings- og asylmyndigheter.

2. Med henblikk på å forebygge, etterforske, avsløre eller straffeforfølge straffbare forhold eller iverksette strafferettslige sanksjoner, herunder beskytte mot og forebygge trusler mot offentlige sikkerhet, under rettshåndhevende myndigheters kontroll og ansvar, skal behandlingen av personopplysninger i regulatoriske sandkasser for KI baseres på særskilt unionsrett eller nasjonal rett og være underlagt de samme kumulative vilkårene som nevnt i nr. 1.

3. Nr. 1 berører ikke unionsrett eller nasjonal rett som forbyr behandling av personopplysninger for andre formål enn dem som er uttrykkelig nevnt i slik rett, og heller ikke unionsrett eller nasjonal rett som fastsetter grunnlaget for behandling av personopplysninger som er nødvendige for å utvikle, teste eller trene innovative KI-systemer, eller noe annet rettsgrunnlag, i samsvar med unionsretten om vern av personopplysninger.

Artikkel 60

Testing av KI-systemer med høy risiko under virkelige forhold utenfor regulatoriske sandkasser for KI

1. Testing av KI-systemer med høy risiko under virkelige forhold utenfor regulatoriske sandkasser for KI kan utføres av leverandører eller prospektive leverandører av KI-systemer med høy risiko som er oppført i vedlegg III, i samsvar med denne artikkelen og med planen for testing under virkelige forhold nevnt i denne artikkelen, uten at det berører forbudene i henhold til artikkel 5.

Kommisjonen skal ved hjelp av gjennomføringsrettsakter spesifisere de nærmere elementene i planen for testing under virkelige forhold. Disse gjennomføringsrettsaktene skal vedtas i samsvar med undersøkelsesprosedyren nevnt i artikkel 98 nr. 2.

Dette nummeret skal ikke berøre unionsrett eller nasjonal rett om testing under virkelige forhold av KI-systemer med høy risiko i forbindelse med produkter som omfattes av EU-harmoniseringsregelverket oppført i vedlegg I.

2. Leverandører eller prospektive leverandører kan gjennomføre testing under virkelige forhold av KI-systemer med høy risiko nevnt i vedlegg III når som helst før de bringer KI-systemet i omsetning eller tar det i bruk på egen hånd eller i samarbeid med en eller flere idriftsettere eller prospektive idriftsettere.

3. Testing under virkelige forhold av KI-systemer med høy risiko i samsvar med denne artikkelen skal ikke berøre en eventuell etisk vurdering som kreves i henhold til unionsretten eller nasjonal rett.

4. Leverandører eller prospektive leverandører kan utføre testing under virkelige forhold bare dersom alle følgende vilkår er oppfylt:

- a) Leverandøren eller den prospektive leverandøren har utarbeidet en plan for testing under virkelige forhold og sendt den til markedstilsynsmyndigheten i den medlemsstaten der testingen under virkelige forhold skal gjennomføres.
- b) Markedstilsynsmyndigheten i den medlemsstaten der testingen under virkelige forhold skal gjennomføres, har godkjent testingen under virkelige forhold og planen for denne; dersom markedstilsynsmyndigheten ikke har svart innen 30 dager, skal testingen under virkelige forhold og planen for denne anses som godkjent; dersom nasjonal rett ikke gir hjemmel for stilltiende godkjenning, skal testingen under virkelige forhold fortsatt være betinget av godkjenning.
- c) Leverandøren eller den prospektive leverandøren, unntatt leverandører eller prospektive leverandører av KI-systemer med høy risiko omhandlet i vedlegg III nr. 1, 6 og 7, på områdene rettshåndhevelse og migrasjons-, asyl- og grensekontrollforvaltning, og unntatt KI-systemer med høy risiko omhandlet i vedlegg III nr. 2, har registrert testingen under virkelige forhold i samsvar med artikkel 71 nr. 4, med et unikt EU-identifikasjonsnummer og med opplysningene angitt i vedlegg IX; leverandøren eller den prospektive leverandøren av KI-systemer med høy risiko omhandlet i vedlegg III nr. 1, 6 og 7, på områdene rettshåndhevelse og migrasjons-, asyl- og grensekontrollforvaltning, har registrert testingen under virkelige forhold i den sikre, ikke-offentlige delen av EU-databasen i samsvar med artikkel 49 nr. 4 bokstav d), med et unikt EU-identifikasjonsnummer og med opplysningene angitt der; leverandøren eller den prospektive leverandøren av KI-systemer med høy risiko omhandlet i vedlegg III nr. 2 har registrert testingen under virkelige forhold i samsvar med artikkel 49 nr. 5.

- d) Leverandøren eller den prospektive leverandøren som utfører testingen under virkelige 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 testingen under virkelige forhold, blir bare overført til tredjeland dersom det er iverksatt egnede og gjeldende sikkerhetstiltak i henhold til unionsretten.
- f) Testingen under virkelige forhold varer ikke lenger enn det som er nødvendig for å nå målene, og i alle tilfeller ikke lenger enn seks måneder, som kan forlenges med en periode på ytterligere seks måneder, forutsatt at leverandøren eller den prospektive leverandøren melder fra til markedstilsynsmyndigheten om dette på forhånd, med en forklaring på hvorfor det er behov for en slik forlengelse.
- g) De forsøkspersonene i testingen under virkelige forhold som tilhører sårbare grupper på grunn av alder eller funksjonsnedsettelse, er tilstrekkelig beskyttet.
- h) Dersom en leverandør eller prospektiv leverandør organiserer testingen under virkelige forhold i samarbeid med en eller flere idriftsettere eller prospektive idriftsettere, er sistnevnte blitt informert om alle aspekter ved testingen som er relevante for deres beslutning om å delta, og gitt den relevante bruksanvisningen for KI-systemet som nevnt i artikkel 13; leverandøren eller den prospektive leverandøren og idriftsetteren eller den prospektive idriftsetteren skal inngå en avtale som spesifiserer deres roller og ansvar, med sikte på å sikre overholdelse av bestemmelsene om testing under virkelige forhold i henhold til denne forordningen og annen gjeldende unionsrett og nasjonal rett.
- i) Forsøkspersonene i testingen under virkelige forhold har gitt informert samtykke i samsvar med artikkel 61, eller, når det gjelder rettshåndhevelse, der innhenting av informert samtykke ville hindret testing av KI-systemet, har verken testingen under virkelige forhold eller resultatene av denne noen negative virkninger for forsøkspersonene, og deres personopplysninger slettes etter at testen er fullført.
- j) Testingen under virkelige forhold overvåkes effektivt av leverandøren eller den prospektive leverandøren samt av idriftsettere eller prospektive idriftsettere gjennom personer som er kvalifisert på det aktuelle feltet og har den nødvendige kapasiteten, opplæringen og myndigheten til å utføre sine oppgaver.
- k) KI-systemets prediksjoner, anbefalinger eller beslutninger kan effektivt reverseres og ignoreres.

5. Alle forsøkspersoner som deltar i testingen under virkelige forhold, eller deres lovlig utpakte representant, kan når som helst, uten negative konsekvenser og uten å måtte gi en begrunnelse, trekke seg fra testingen ved å trekke tilbake det informerte samtykket og kan be om umiddelbar og permanent sletting av personopplysningene sine. Tilbaketrekking av det informerte samtykket skal ikke påvirke de aktivitetene som allerede er gjennomført.

6. I samsvar med artikkel 75 skal medlemsstatene gi sine markedstilsynsmyndigheter fullmakt til å pålegge leverandører og prospektive leverandører å framlegge opplysninger, til å utføre uanmeldte fjerninspeksjoner eller inspeksjoner på stedet og til å kontrollere gjennomføringen av testingen under virkelige forhold og de tilknyttede KI-systemene med høy risiko. Markedstilsynsmyndighetene skal bruke disse fullmaktene til å sørge for sikker utvikling av testing under virkelige forhold.

7. Enhver alvorlig hendelse som avdekkes under testing under virkelige forhold, skal rapporteres til den nasjonale markedstilsynsmyndigheten i samsvar med artikkel 73. Leverandøren eller den prospektive leverandøren skal treffe umiddelbare risikoreduerende tiltak eller, dersom dette ikke er mulig, suspendere testingen under virkelige forhold til slik risikoreduksjon finner sted, eller i motsatt fall avslutte den. Leverandøren eller den prospektive leverandøren skal fastsette en prosedyre for rask tilbaketrekking av KI-systemet når testing under virkelige forhold avsluttes på denne måten.

8. Leverandører eller prospektive leverandører skal underrette den nasjonale markedstilsynsmyndigheten i den medlemsstaten der testingen under virkelige forhold gjennomføres, om at testingen er suspendert eller avsluttet, og om de endelige resultatene.

9. Leverandøren eller den prospektive leverandøren skal være ansvarlig i henhold til gjeldende unionsrett og nasjonal rett om erstatningsansvar for eventuelle skader som oppstår under dennes testing under virkelige forhold.

Artikkel 61

Informert samtykke til å delta i testing under virkelige forhold utenfor regulatoriske sandkasser for KI

1. Med henblikk på testing under virkelige forhold i henhold til artikkel 60 skal det innhentes fritt avgitt informert samtykke fra forsøkspersonene før de deltar i slik testing, og etter at de på kortfattet, klar, relevant og forståelig måte er blitt behørig informert om
 - a) arten av og målene for testingen under virkelige forhold og de mulige ulempene som deltakelsen kan medføre,
 - b) omstendighetene rundt gjennomføringen av testingen under virkelige forhold, herunder hvor lenge forsøkspersonens eller forsøkspersonenes deltakelse forventes å vare,
 - c) sine rettigheter og garantier i forbindelse med deres deltakelse, særlig retten til å nekte å delta i og når som helst å trekke seg fra testingen under virkelige forhold uten at dette får negative konsekvenser, og uten at de må begrunne det,
 - d) ordningene for å be om å reversere eller ignorere KI-systemets prediksjoner, anbefalinger eller beslutninger,
 - e) det unike EU-identifikasjonsnummeret for testing under virkelige forhold i samsvar med artikkel 60 nr. 4 bokstav c) og kontaktopplysningene til leverandøren eller dennes juridiske representant som det kan innhentes ytterligere opplysninger fra.
2. Det informerte samtykket skal være datert og dokumentert, og det skal gis en kopi til forsøkspersonene eller deres juridiske representant.

Artikkel 62

Tiltak for leverandører og idriftsettere, særlig små og mellomstore bedrifter, herunder oppstartsbedrifter

1. Medlemsstatene skal
 - a) gi små og mellomstore bedrifter, herunder oppstartsbedrifter, som har et forretningskontor eller en filial i Unionen, prioritert tilgang til de regulatoriske sandkassene for KI, forutsatt at de oppfyller kvalifikasjonsvilkårene og utvelgelseskriteriene; den prioriterte tilgangen skal ikke hindre andre små og mellomstore bedrifter, herunder oppstartsbedrifter, enn dem som omhandles i dette nummeret, i å få tilgang til den regulatoriske sandkassen for KI, forutsatt at også de oppfyller kvalifikasjonsvilkårene og utvelgelseskriteriene,
 - b) organisere særlige bevisstgjørings- og opplæringsaktiviteter om anvendelsen av denne forordningen, tilpasset behovene til små og mellomstore bedrifter, herunder oppstartsbedrifter, idriftsettere og, dersom det er relevant, lokale offentlige myndigheter,
 - c) benytte eksisterende særskilte kanaler, og ved behov opprette nye, til å kommunisere med små og mellomstore bedrifter, herunder oppstartsbedrifter, samt idriftsettere, andre innovatører og, dersom det er relevant, lokale offentlige myndigheter, for å gi råd og svare på spørsmål om gjennomføringen av denne forordningen, herunder med hensyn til deltakelse i regulatoriske sandkasser for KI,
 - d) legge til rette for at små og mellomstore bedrifter og andre relevante berørte parter kan delta i prosessen for utarbeiding av standarder.
2. Det skal tas hensyn til de særlige interessene og behovene til leverandører som er små og mellomstore bedrifter, herunder oppstartsbedrifter, når gebyrene for samsvarsvurdering fastsettes i henhold til artikkel 43, og gebyrene skal reduseres proporsjonalt med deres størrelse, markedsstørrelsen og andre relevante indikatorer.
3. KI-kontoret skal
 - a) levere standardiserte maler for områder som omfattes av denne forordningen, som angitt av KI-rådet i dets anmodning,
 - b) utvikle og vedlikeholde en felles informasjonsplattform som gir brukervennlig informasjon om denne forordningen til alle operatører i Unionen,

- c) organisere egnede informasjonskampanjer for å øke bevisstheten om de forpliktelsene som følger av denne forordningen,
- d) evaluere og fremme tilnærming av beste praksis i offentlige anskaffelsesprosedyrer med hensyn til KI-systemer.

Artikkel 63

Unntak for bestemte operatører

1. Svært små bedrifter som definert i rekommandasjon 2003/361/EF kan overholde visse elementer i kvalitetsstyringssystemet som kreves i henhold til artikkel 17 i denne forordningen, på en forenklet måte, forutsatt at de ikke har partnerforetak eller tilknyttede foretak som definert i nevnte rekommandasjon. For dette formålet skal Kommisjonen utarbeide retningslinjer for de elementene i kvalitetsstyringssystemet som kan overholdes på en forenklet måte, i betraktning av behovene til svært små bedrifter, uten at det påvirker vernenivået eller nødvendigheten av å oppfylle kravene til KI-systemer med høy risiko.
2. Nr. 1 i denne artikkelen skal ikke tolkes slik at disse operatørene fritas for å oppfylle andre krav eller forpliktelser fastsatt i denne forordningen, herunder dem som er fastsatt i artikkel 9, 10, 11, 12, 13, 14, 15, 72 og 73.

KAPITTEL VII

FORVALTNING

AVSNITT 1

Forvaltning på unionsplan

Artikkel 64

KI-kontoret

1. Kommisjonen skal utvikle Unionens ekspertise og kapabiliteter på KI-området gjennom KI-kontoret.
2. Medlemsstatene skal lette de oppgavene som er gitt til KI-kontoret, som avspeilet i denne forordningen.

Artikkel 65

Opprettelse og sammensetning av Det europeiske rådet for kunstig intelligens

1. Det opprettes herved et europeisk råd for kunstig intelligens («KI-rådet»).
2. KI-rådet skal være sammensatt av én representant for hver medlemsstat. EUs datatilsyn skal delta som observatør. KI-kontoret skal også delta på KI-rådets møter, uten å delta i avstemningene. KI-rådet kan fra tilfelle til tilfelle invitere andre myndigheter, organer eller eksperter på nasjonalt plan eller unionsplan til møtene dersom spørsmålene som drøftes, er av betydning for dem.
3. Hver representant skal utpekes av sin medlemsstat for et tidsrom på tre år som kan fornyes én gang.
4. Medlemsstatene skal sikre at deres representanter i KI-rådet
 - a) har den relevante kompetansen og de relevante fullmaktene i sin medlemsstat til å kunne bidra aktivt til utførelsen av KI-rådets oppgaver som nevnt i artikkel 66,
 - b) utpekes som et felles kontaktpunkt overfor KI-rådet og, dersom det er relevant, idet det tas hensyn til medlemsstatenes behov, som et felles kontaktpunkt for berørte parter,

- c) har myndighet til å legge til rette for samsvar og samordning mellom nasjonale vedkommende myndigheter i sin medlemsstat med hensyn til gjennomføringen av denne forordningen, herunder gjennom innhenting av relevante data og opplysninger for å kunne utføre sine oppgaver i KI-rådet.

5. Medlemsstatenes utpekte representanter skal vedta KI-rådets forretningsorden med to tredels flertall. Forretningsordenen skal særlig fastsette prosedyrer for utvelgelsesprosessen, varigheten av lederens mandat og spesifikasjonen av lederens oppgaver, de nærmere avstemningsreglene og organiseringen av virksomheten til KI-rådet og dets undergrupper.

6. KI-rådet skal opprette to faste undergrupper for å skape en plattform for samarbeid og utveksling mellom markedstilsynsmyndigheter og meldermyndigheter om spørsmål knyttet til henholdsvis markedstilsyn og meldte organer.

Den faste undergruppen for markedstilsyn bør fungere som den administrative samarbeidsgruppen for denne forordningen i henhold til artikkel 30 i forordning (EU) 2019/1020.

KI-rådet kan opprette andre faste eller midlertidige undergrupper etter behov for å behandle særlige spørsmål. Dersom det er relevant, kan representanter for det rådgivende forumet nevnt i artikkel 67 inviteres til slike undergrupper eller til bestemte møter i disse undergruppene som observatører.

7. KI-rådet skal være organisert og drives på en slik måte at det sikres objektivitet og upartiskhet i dets virksomhet.

8. KI-rådet skal ledes av en av representantene for medlemsstatene. KI-kontoret skal fungere som KI-rådets sekretariat, sammenkalle møtene på lederens anmodning og utarbeide dagsordenen i samsvar med KI-rådets oppgaver etter denne forordningen samt dets forretningsorden.

Artikkel 66

KI-rådets oppgaver

KI-rådet skal gi råd til og bistå Kommisjonen og medlemsstatene for å lette en konsekvent og effektiv anvendelse av denne forordningen. For dette formålet kan KI-rådet særlig

- a) bidra til samordning mellom de nasjonale vedkommende myndighetene med ansvar for anvendelsen av denne forordningen og støtte felles aktiviteter blant markedstilsynsmyndigheter som omhandlet i artikkel 74 nr. 11, i samarbeid med og med samtykke fra de aktuelle markedstilsynsmyndighetene,
- b) innhente og dele teknisk og regulatorisk ekspertise og beste praksis mellom medlemsstatene,
- c) gi råd om gjennomføringen av denne forordningen, særlig når det gjelder håndhevelse av regler om KI-modeller for allmenne formål,
- d) bidra til harmonisering av den administrative praksisen i medlemsstatene, herunder i forbindelse med unntakene fra samsvarsvurderingsprosedyren omhandlet i artikkel 46, virkemåten til de regulatoriske sandkassene for KI og testingen under virkelige forhold omhandlet i artikkel 57, 59 og 60,
- e) på anmodning fra Kommisjonen eller på eget initiativ utstede anbefalinger og skriftlige uttalelser om alle relevante spørsmål knyttet til gjennomføringen av denne forordningen og konsekvent og effektiv anvendelse av den, herunder:
 - i) utarbeiding og anvendelse av atferdsregler og regler for god praksis i samsvar med denne forordningen og av Kommisjonens retningslinjer,
 - ii) evaluering og revisjon av denne forordningen i samsvar med artikkel 112, herunder når det gjelder rapportene om alvorlige hendelser omhandlet i artikkel 73 og virkemåten til EU-databasen omhandlet i artikkel 71, utarbeiding av de legerte rettsakter eller gjennomføringsrettsakter og mulige tilpasninger av denne forordningen til EU-harmoniseringsregelverket oppført i vedlegg I,
 - iii) tekniske spesifikasjoner eller eksisterende standarder med hensyn til kravene i kapittel III avsnitt 2,

- iv) bruk av harmoniserte standarder eller felles spesifikasjoner som omhandlet i artikkel 40 og 41,
- v) trender, for eksempel i europeisk global konkurranseevne innen KI, utbredelse av KI i Unionen og utvikling av digitale ferdigheter,
- vi) trender i utviklingen av typologien i KI-verdikjeder, særlig konsekvensene når det gjelder ansvarlighet,
- vii) det potensielle behovet for å endre vedlegg III i samsvar med artikkel 7 og for å revidere artikkel 5 i samsvar med artikkel 112, i betraktning av relevant tilgjengelig dokumentasjon og den siste teknologiske utviklingen,
- f) støtte Kommisjonen i å fremme verktøy for KI-kompetanse og allmennhetens kjennskap til og forståelse av fordeler, risikoer, sikkerhetstiltak, rettigheter og forpliktelser ved bruk av KI-systemer,
- g) lette utarbeidingen av felles kriterier og en felles forståelse av de relevante begrepene i denne forordningen blant markedsaktører og vedkommende myndigheter, herunder ved å bidra til utarbeiding av referanseverdier,
- h) samarbeide, alt etter hva som er relevant, med andre EU-institusjoner, -organer, -kontorer og -byråer samt relevante EU-ekspertgrupper og -nettverk, særlig på områdene produktsikkerhet, cybersikkerhet, konkurranse, digitale tjenester og medietjenester, finansielle tjenester, forbrukervern, databeskyttelse og beskyttelse av grunnleggende rettigheter,
- i) bidra til effektivt samarbeid med vedkommende myndigheter i tredjeland og med internasjonale organisasjoner,
- j) bistå nasjonale vedkommende myndigheter og Kommisjonen med å opparbeide den organisatoriske og tekniske ekspertisen som er nødvendig for gjennomføringen av denne forordningen, herunder ved å bidra i vurderingen av opplæringsbehovet hos personale i medlemsstatene som er involvert i gjennomføringen av denne forordningen,
- k) bistå KI-kontoret med å støtte nasjonale vedkommende myndigheter i opprettelsen og utviklingen av regulatoriske sandkasser for KI og legge til rette for samarbeid og informasjonsdeling mellom regulatoriske sandkasser for KI,
- l) bidra til og gi relevante råd om utarbeiding av veiledningsdokumenter,
- m) gi råd til Kommisjonen i internasjonale KI-spørsmål,
- n) gi uttalelser til Kommisjonen om kvalifiserte varsler om KI-modeller for allmenne formål,
- o) motta uttalelser fra medlemsstatene om kvalifiserte varsler om KI-modeller for allmenne formål og om nasjonale erfaringer og nasjonal praksis med hensyn til overvåking og håndhevelse av KI-systemer, særlig systemer som integrerer KI-modellene for allmenne formål.

Artikkel 67

Rådgivende forum

1. Det skal opprettes et rådgivende forum som skal yte teknisk ekspertise og gi råd til KI-rådet og Kommisjonen og bidra til deres oppgaver i henhold til denne forordningen.
2. Medlemskapet i det rådgivende forumet skal representere et balansert utvalg av berørte parter, herunder industri, oppstartsbedrifter, små og mellomstore bedrifter, sivilsamfunnet og academia. Medlemskapet i det rådgivende forum skal være balansert mellom kommersielle og ikke-kommersielle interesser og, i kategorien kommersielle interesser, mellom små og mellomstore bedrifter og andre foretak.
3. Kommisjonen skal utnevne medlemmene av det rådgivende forumet, i samsvar med kriteriene nevnt i nr. 2, blant berørte parter med anerkjent ekspertise på KI-området.

4. Mandatperioden for medlemmene i det rådgivende forumet skal være to år, som kan forlenges med høyst fire år.
5. Byrådet for grunnleggende rettigheter (ENISA), Den europeiske standardiseringsorganisasjon (CEN), Den europeiske komité for elektroteknisk standardisering (CENELEC) og Det europeiske standardiseringsinstitutt for telekommunikasjon (ETSI) skal være faste medlemmer i det rådgivende forumet.
6. Det rådgivende forumet fastsetter sin forretningsorden. Det skal velge to medledere blant sine medlemmer, i samsvar med kriteriene nevnt i nr. 2. Medlederens mandatperiode skal være på to år, som kan forlenges én gang.
7. Det rådgivende forumet skal tre sammen minst to ganger i året. Det rådgivende forumet kan invitere eksperter og andre berørte parter til sine møter.
8. Det rådgivende forumet kan utarbeide uttalelser, anbefalinger og skriftlige bidrag på anmodning fra KI-rådet eller Kommisjonen.
9. Det rådgivende forumet kan etter behov opprette faste eller midlertidige undergrupper for å behandle særlige spørsmål knyttet til denne forordningens mål.
10. Det rådgivende forumet skal utarbeide en årsrapport om sin virksomhet. Rapporten skal offentliggjøres.

Artikkel 68

Vitenskapspanel av uavhengige eksperter

1. Kommisjonen skal ved en gjennomføringsrettsakt fastsette bestemmelser om opprettelse av et vitenskapspanel av uavhengige eksperter («vitenskapspanelet») som skal støtte håndhevelsesvirksomheten i henhold til denne forordningen. Denne gjennomføringsrettsakten skal vedtas i samsvar med undersøkelsesprosedyren nevnt i artikkel 98 nr. 2.
2. Vitenskapspanelet skal bestå av eksperter som Kommisjonen velger ut på grunnlag av oppdatert vitenskapelig eller teknisk ekspertise på KI-området som er nødvendig for oppgavene nevnt i nr. 3, og som kan dokumentere at de oppfyller alle følgende vilkår:
 - a) De har særlig ekspertise og kompetanse samt vitenskapelig eller teknisk sakkunnskap på KI-området.
 - b) De er uavhengige av enhver leverandør av KI-systemer eller av KI-modeller for allmenne formål.
 - c) De har evne til å utføre aktiviteter med aktsomhet, nøyaktighet og objektivitet.

Kommisjonen skal i samråd med KI-rådet fastsette antallet eksperter i panelet ut fra behovene og skal sikre en rettferdig kjønnsmessig og geografisk representasjon.
3. Vitenskapspanelet skal gi råd og støtte til KI-kontoret, særlig med hensyn til følgende oppgaver:
 - a) støtte gjennomføring og håndhevelse av denne forordningen med hensyn til KI-modeller og -systemer for allmenne formål, særlig ved å
 - i) varsle KI-kontoret om mulig systemrisiko på unionsplan ved KI-modeller for allmenne formål, i samsvar med artikkel 90,
 - ii) bidra til utvikling av verktøy og metoder for å evaluere kapabilitetene til KI-modeller og -systemer for allmenne formål, blant annet gjennom referanseverdier,
 - iii) gi råd om klassifisering av KI-modeller for allmenne formål med systemrisiko,
 - iv) gi råd om klassifisering av ulike KI-modeller og -systemer for allmenne formål,

- v) bidra til utvikling av verktøy og maler,
 - b) støtte arbeidet til markedstilsynsmyndighetene, på deres anmodning,
 - c) støtte markedstilsynsaktiviteter over landegrensene som nevnt i artikkel 74 nr. 11, uten at det berører markedstilsynsmyndighetenes fullmakter,
 - d) støtte KI-kontoret i utførelsen av deres oppgaver innenfor rammen av EU-beskyttelsesprosedyren i samsvar med artikkel 81.
4. Ekspertene i vitenskapspanelet skal utføre sine oppgaver på en upartisk og objektiv måte og skal sikre fortrolig behandling av opplysninger og data som de mottar når de utfører sine oppgaver og sin virksomhet. De skal verken be om eller motta instruksjoner fra noen når de utfører sine oppgaver i henhold til nr. 3. Hver ekspert skal avgi en interesseerklæring som skal gjøres offentlig tilgjengelig. KI-kontoret skal opprette systemer og prosedyrer for aktivt å håndtere og forebygge potensielle interessekonflikter.
5. Gjennomføringsrettsakten nevnt i nr. 1 skal inneholde bestemmelser om vilkårene, prosedyrene og de nærmere ordningene for at vitenskapspanelet og dets medlemmer kan utstede varsler og be om bistand fra KI-kontoret til utførelsen av vitenskapspanelet oppgaver.

Artikkel 69

Medlemsstatenes tilgang til gruppen av eksperter

1. Medlemsstatene kan anmode eksperter fra vitenskapspanelet om støtte til sine håndhevelsesaktiviteter i henhold til denne forordningen.
2. Medlemsstatene kan bli pålagt å betale gebyrer for råd og støtte fra ekspertene. Gebyrenes struktur og nivå samt omfanget av og strukturen på de kostnadene som kan kreves erstattet, skal fastsettes i gjennomføringsrettsakten nevnt i artikkel 68 nr. 1, idet det tas hensyn til målene om korrekt gjennomføring av denne forordningen, kostnadseffektivitet og nødvendigheten av å sikre effektiv tilgang til eksperter for alle medlemsstater.
3. Kommisjonen skal legge til rette for at medlemsstatene etter behov får tilgang til ekspertene i rett tid, og sikre at kombinasjonen av støtteaktiviteter som utføres av EU-støttestrukturene for KI-testing i henhold til artikkel 84 og av eksperter i henhold til denne artikkelen, er effektivt organisert og gir best mulig merverdi.

AVSNITT 2

Nasjonale vedkommende myndigheter

Artikkel 70

Utpeking av nasjonale vedkommende myndigheter og et felles kontaktpunkt

1. Hver medlemsstat skal opprette eller utpeke minst én meldermyndighet og minst én markedstilsynsmyndighet som nasjonale vedkommende myndigheter for denne forordningens formål. Disse nasjonale vedkommende myndighetene skal utøve sine fullmakter på en uavhengig, upartisk måte og uten forutinntatthet for å sikre objektivitet i sine aktiviteter og oppgaver, og for å sørge for at denne forordningen anvendes og gjennomføres. Disse myndighetenes medlemmer skal avholde seg fra enhver handling som er uforenlig med deres verv. Forutsatt at disse prinsippene overholdes, kan slike aktiviteter og oppgaver utføres av én eller flere utpekte myndigheter, alt etter 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 innen 2. august 2025 gjøre informasjon offentlig tilgjengelig om hvordan de vedkommende myndighetene og felles kontaktpunktene kan kontaktes ved hjelp av elektroniske kommunikasjonsmidler. Medlemsstatene skal utpeke en markedstilsynsmyndighet som skal fungere som felles kontaktpunkt for denne forordningen, og underrette Kommisjonen om identiteten til det felles kontaktpunktet. Kommisjonen skal gjøre en liste over de felles kontaktpunktene offentlig tilgjengelig.

3. Medlemsstatene skal sikre at deres nasjonale vedkommende myndigheter har tilstrekkelige tekniske, økonomiske og menneskelige ressurser og infrastruktur til å kunne utføre sine oppgaver effektivt i henhold til denne forordningen. Framfor alt skal de nasjonale vedkommende myndighetene ha permanent tilgang til et tilstrekkelig antall ansatte med kompetanse og ekspertise som omfatter en inngående forståelse av KI-teknologier, data og databehandling, vern av personopplysninger, cybersikkerhet, 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 nummeret en gang i året.
4. Nasjonale vedkommende myndigheter skal treffe egnede tiltak for å sikre et tilstrekkelig nivå av cybersikkerhet.
5. Når de utfører sine oppgaver, skal de nasjonale vedkommende myndighetene opptre i samsvar med fortrolighetsforpliktelsene fastsatt i artikkel 78.
6. Innen 2. august 2025 og deretter en gang hvert andre år skal medlemsstatene rapportere til Kommisjonen om statusen for de nasjonale vedkommende myndighetenes økonomiske og menneskelige ressurser, med en vurdering av om de er tilstrekkelige. Kommisjonen skal oversende disse opplysningene til KI-rådet for drøfting og eventuelle anbefalinger.
7. Kommisjonen skal lette utveksling av erfaringer mellom nasjonale vedkommende myndigheter.
8. Nasjonale vedkommende myndigheter kan gi veiledning og råd om gjennomføringen av denne forordningen, særlig til små og mellomstore bedrifter, herunder oppstartsbedrifter, idet det tas hensyn til veiledningen og rådene fra KI-rådet og Kommisjonen, alt etter hva som er relevant. Når nasjonale vedkommende myndigheter har til hensikt å gi veiledning og råd om et KI-system på områder som omfattes av annen unionsrett, skal det holdes samråd med de nasjonale vedkommende myndighetene i henhold til den unionsretten, alt etter hva som er relevant.
9. Når Unionens institusjoner, organer, kontorer eller byråer omfattes av denne forordningens virkeområde, skal EUs datatilsyn fungere som vedkommende myndighet for tilsynet med dem.

KAPITTEL VIII

EU-DATABASE FOR KI-SYSTEMER MED HØY RISIKO

Artikkel 71

EU-database for KI-systemer med høy risiko oppført i vedlegg III

1. Kommisjonen skal i samarbeid med medlemsstatene opprette og vedlikeholde en EU-database som inneholder opplysningene nevnt i nr. 2 og 3 i denne artikkelen om KI-systemer med høy risiko som nevnt i artikkel 6 nr. 2 som er registrert i samsvar med artikkel 49 og 60, og KI-systemer som ikke anses å ha høy risiko i henhold til artikkel 6 nr. 3, og som er registrert i samsvar med artikkel 6 nr. 4 og artikkel 49. Når Kommisjonen fastsetter funksjonsspesifikasjonene for en slik database, skal den rådføre seg med de relevante ekspertene, og når den oppdaterer funksjonsspesifikasjonene for en slik database, skal den rådføre seg med KI-rådet.
2. Dataene oppført i avsnitt A og B i vedlegg VIII skal legges inn i EU-databasen av leverandøren eller, dersom det er relevant, av den bemyndigede representanten.
3. Dataene oppført i vedlegg VIII avsnitt C skal legges inn i EU-databasen av den idriftsetteren som er, eller som opptrer på vegne av, en offentlig myndighet eller et offentlig byrå eller 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 de opplysningene i EU-databasen som er registrert i samsvar med artikkel 49, være tilgjengelige for allmennheten på en brukervennlig måte. Opplysningene bør være lette å navigere i og maskinlesbare. De opplysningene som er registrert i samsvar med artikkel 60, skal være tilgjengelige bare for markedstilsynsmyndigheter og Kommisjonen, med mindre leverandøren eller den prospektive leverandøren har gitt samtykke til også å gjøre opplysningene 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 forordningen. Disse opplysningene skal omfatte navn på og kontaktopplysninger til fysiske personer som er ansvarlige for å registrere systemet, og som har rettslig myndighet til å representere leverandøren eller idriftsetteren, alt etter hva som er relevant.

6. Kommisjonen skal være behandlingsansvarlig for EU-databasen. Den skal gjøre tilstrekkelig teknisk og administrativ støtte tilgjengelig for leverandører, prospektive leverandører og idriftsettere. EU-databasen skal oppfylle de gjeldende tilgjengelighetskravene.

KAPITTEL IX

OVERVÅKING ETTER OMSETNING, INFORMASJONSDELING OG MARKEDSTILSYN

AVSNITT 1

Overvåking etter omsetning

Artikkel 72

Leverandørers overvåking etter omsetning og plan for overvåking etter omsetning av KI-systemer med høy risiko

1. Leverandørene skal opprette og dokumentere et system for overvåking etter omsetning på en måte som står i forhold til KI-teknologienes art og risikoene ved KI-systemet med høy risiko.

2. Systemet for overvåking etter omsetning skal aktivt og systematisk samle inn, dokumentere og analysere relevante data som kan leveres av idriftsettere eller samles inn via andre kilder, om ytelsen til KI-systemene med høy risiko i hele deres levetid, og som gjør det mulig for leverandøren å evaluere KI-systemenes løpende overholdelse av kravene i kapittel III avsnitt 2. Dersom det er relevant, skal overvåkingen etter omsetning omfatte en analyse av samhandlingen med andre KI-systemer. Denne forpliktelsen omfatter ikke sensitive operasjonelle data tilhørende idriftsettere som er rettshåndhevende myndigheter.

3. Systemet for overvåking etter omsetning skal bygge på en plan for overvåking etter omsetning. Planen for overvåking etter omsetning skal være en del av den tekniske dokumentasjonen omhandlet i vedlegg IV. Kommisjonen skal innen 2. februar 2026 vedta en gjennomføringsrettsakt som fastsetter nærmere bestemmelser om opprettelse av en mal for planen for overvåking etter omsetning, og de elementene som skal inngå i planen. Denne gjennomføringsrettsakten skal vedtas i samsvar med undersøkelsesprosedyren nevnt i artikkel 98 nr. 2.

4. For KI-systemer med høy risiko som omfattes av EU-harmoniseringsregelverket oppført i avsnitt A i vedlegg I, og der det allerede er opprettet et system og en plan for overvåking etter omsetning i henhold nevnte regelverk, skal leverandørene, for å sikre konsekvens, unngå dobbeltarbeid og redusere tilleggsbyrdene mest mulig, ha mulighet til å velge, alt etter hva som er relevant, å integrere de nødvendige elementene beskrevet i nr. 1, 2 og 3 ved bruk av malen nevnt i nr. 3, i systemer og planer som allerede foreligger i henhold til nevnte regelverk, forutsatt at den oppnår et tilsvarende vernnivå.

Første ledd i dette nummeret skal også gjelde for KI-systemer med høy risiko omhandlet i vedlegg III nr. 5 som bringes i omsetning eller tas i bruk av finansinstitusjoner som er underlagt krav i unionsretten om finansielle tjenester med hensyn til deres interne styreformer, ordninger eller prosesser.

AVSNITT 2

Deling av opplysninger om alvorlige hendelser

Artikkel 73

Rapportering av alvorlige hendelser

1. Leverandører av KI-systemer med høy risiko som bringes i omsetning på unionsmarkedet, skal rapportere enhver alvorlig hendelse til markedstilsynsmyndighetene i de medlemsstatene der hendelsen har inntruffet.

2. Rapporteringen nevnt i nr. 1 skal skje umiddelbart etter at leverandøren har fastslått en årsakssammenheng mellom KI-systemet og den alvorlige hendelsen eller en rimelig sannsynlighet for en slik sammenheng, og i alle tilfeller senest 15 dager etter at leverandøren eller, dersom det er relevant, idriftsetteren har fått kjennskap til den alvorlige hendelsen.

Rapporteringsfristen nevnt i første ledd skal ta hensyn til hvor alvorlig hendelsen er.

3. Uten hensyn til nr. 2 i denne artikkelen skal rapporteringen nevnt i nr. 1 i denne artikkelen ved en utbredt overtredelse eller en alvorlig hendelse som definert i artikkel 3 nr. 49 bokstav b) skje umiddelbart og senest to dager etter at leverandøren eller, dersom det er relevant, idriftsetteren får kjennskap til hendelsen.

4. Uten hensyn til nr. 2 skal rapporteringen ved dødsfall skje umiddelbart etter at leverandøren eller idriftsetteren har fastslått eller har fått mistanke om at det er en årsakssammenheng mellom KI-systemet med høy risiko og den alvorlige hendelsen, men senest ti dager etter at leverandøren eller, dersom det er relevant, idriftsetteren får kjennskap til den alvorlige hendelsen.

5. Dersom det er nødvendig for å sikre rettidig rapportering, kan leverandøren eller, dersom det er relevant, idriftsetteren levere en innledende rapport som ikke er fullstendig, og deretter en fullstendig rapport.

6. Etter å ha rapportert en alvorlig hendelse i samsvar med nr. 1 skal produsenten umiddelbart foreta de nødvendige undersøkelsene i forbindelse med den alvorlige hendelsen og det KI-systemet det gjelder. Dette skal omfatte en risikovurdering av hendelsen og korrigerende tiltak.

Under undersøkelsene nevnt i første ledd skal leverandøren samarbeide med vedkommende myndigheter og, dersom det er relevant, med det relevante meldte organet og skal ikke foreta undersøkelser som innebærer at det aktuelle KI-systemet endres på en slik måte at det kan påvirke eventuelle etterfølgende vurderinger av årsakene til hendelsen, uten først å underrette vedkommende myndigheter om dette.

7. Når den relevante markedstilsynsmyndigheten mottar en melding om en alvorlig hendelse som nevnt i artikkel 3 nr. 49 bokstav c), skal den underrette de nasjonale offentlige myndighetene eller organene nevnt i artikkel 77 nr. 1. Kommisjonen skal utarbeide særskilt veiledning for å lette oppfyllelsen av forpliktelsene fastsatt i nr. 1 i denne artikkelen. Denne veiledningen skal utstedes innen 2. august 2025 og skal vurderes regelmessig.

8. Markedstilsynsmyndigheten skal treffe egnede tiltak i samsvar med artikkel 19 i forordning (EU) 2019/1020 innen sju dager fra den datoen den mottar meldingen nevnt i nr. 1 i denne artikkelen, og skal følge prosedyrene for underretning fastsatt i nevnte forordning.

9. For KI-systemer med høy risiko omhandlet i vedlegg III som bringes i omsetning eller tas i bruk av leverandører som omfattes av unionsrettsakter der det fastsettes tilsvarende rapporteringsforpliktelser som i denne forordningen, skal meldingen om alvorlige hendelser begrenses til dem som er omhandlet i artikkel 3 nr. 49 bokstav c).

10. For KI-systemer med høy risiko som er sikkerhetskomponenter i utstyr eller selv er utstyr som omfattes av forordning (EU) 2017/745 og (EU) 2017/746, skal meldingen om alvorlige hendelser begrenses til dem som er nevnt i artikkel 3 nr. 49 bokstav c) i denne forordningen, og skal sendes til den nasjonale vedkommende myndigheten som er valgt for dette formålet av medlemsstatene der hendelsen har inntruffet.

11. De nasjonale vedkommende myndighetene skal umiddelbart underrette Kommisjonen om enhver alvorlig hendelse, uansett om de har truffet tiltak i forbindelse med hendelsen eller ikke, i samsvar med artikkel 20 i forordning (EU) 2019/1020.

AVSNITT 3

Håndhevelse

Artikkel 74

Markedstilsyn og kontroll av KI-systemer på unionsmarkedet

1. Forordning (EF) nr. 2019/1020 får anvendelse på KI-systemer som omfattes av denne forordningen. For å sikre effektiv håndhevelse av denne forordningen skal

- a) enhver henvisning til en markedsdeltaker i henhold til forordning (EU) 2019/1020 forstås å omfatte alle operatører angitt i artikkel 2 nr. 1 i denne forordningen,
- b) enhver henvisning til et produkt i henhold til forordning (EU) 2019/1020 forstås å omfatte alle KI-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 alle opplysninger som er identifisert i forbindelse med markedstilsynsaktiviteter, og som kan være av interesse for anvendelsen av unionsretten om konkurranseregler. De skal også årlig rapportere til Kommisjonen om bruk til forbudt praksis som har funnet sted i løpet av det året, og om tiltakene som er truffet.

3. Når det gjelder KI-systemer med høy risiko som er knyttet til produkter som omfattes av EU-harmoniseringsregelverket oppført i avsnitt A i vedlegg I, skal markedstilsynsmyndigheten for denne forordningens formål være den myndigheten som er utpekt som ansvarlig for markedstilsynsaktiviteter i henhold til disse rettsaktene.

Som unntak fra første ledd og under egnede omstendigheter kan medlemsstatene utpeke en annen relevant myndighet til å fungere som markedstilsynsmyndighet, forutsatt at de sikrer samordning med de relevante sektorspesifikke markedstilsynsmyndighetene som har ansvar for håndhevelsen av EU-harmoniseringsregelverket oppført i vedlegg I.

4. Prosedyrene omhandlet i artikkel 79–83 i denne forordningen får ikke anvendelse på KI-systemer som er knyttet til produkter som omfattes av EU-harmoniseringsregelverket oppført i avsnitt A i vedlegg I, dersom det i disse rettsaktene allerede er fastsatt prosedyrer som sikrer et tilsvarende vernnivå, og som har samme mål. I slike tilfeller får de relevante sektorspesifikke prosedyrene anvendelse i stedet.

5. Uten at det berører markedstilsynsmyndighetenes fullmakter i henhold til artikkel 14 i forordning (EU) 2019/1020, kan markedstilsynsmyndighetene, for å sikre effektiv håndhevelse av denne forordningen, utøve fullmaktene nevnt i artikkel 14 nr. 4 bokstav d) og j) i nevnte forordning på avstand, alt etter hva som er relevant.

6. For KI-systemer med høy risiko som bringes i omsetning, tas i bruk eller brukes av finansinstitusjoner som er regulert av unionsretten om finansielle tjenester, skal markedstilsynsmyndigheten for denne forordningens formål være den relevante nasjonale myndigheten med ansvar for det finansielle tilsynet med disse institusjonene i henhold til nevnte rett, dersom KI-systemet bringes i omsetning, tas i bruk eller brukes i direkte forbindelse med leveringen av disse finansielle tjenestene.

7. Som unntak fra nr. 6 kan medlemsstaten under egnede omstendigheter og forutsatt at det sikres samordning, utpeke en annen relevant myndighet som markedstilsynsmyndighet for denne forordningens formål.

Nasjonale markedstilsynsmyndigheter som fører tilsyn med kredittinstitusjoner som er regulert i henhold til direktiv 2013/36/EU, og som deltar i den felles tilsynsordningen opprettet ved rådsforordning (EU) nr. 1024/2013, bør uten ugrunnet opphold rapportere til Den europeiske sentralbank alle opplysninger identifisert i forbindelse med deres markedstilsynsaktiviteter som kan være av interesse for Den europeiske sentralbanks tilsynsoppgaver som angitt i nevnte forordning.

8. For KI-systemer med høy risiko oppført i nr. 1 i vedlegg III til denne forordningen, dersom systemene brukes til retts håndhevelsesformål, grenseforvaltning eller rettspleie og demokratiske prosesser, og for KI-systemer med høy risiko oppført i nr. 6, 7 og 8 i vedlegg III til denne forordningen skal medlemsstatene utpeke enten de vedkommende tilsynsmyndighetene for personvern i henhold til forordning (EU) 2016/679 eller direktiv (EU) 2016/680, eller enhver annen myndighet som er utpekt i henhold til de samme vilkårene fastsatt i artikkel 41–44 i direktiv (EU) 2016/680, som markedstilsynsmyndighet for denne forordningens formål. Markedstilsynsaktiviteter skal ikke på noen måte påvirke rettsmyndighetenes uavhengighet eller på annen måte gripe inn i deres virksomhet når de opptrer innenfor rammen av sin domsmyndighet.

9. Når Unionens institusjoner, organer, kontorer eller byråer faller inn under denne forordningens virkeområde, skal EUs datatilsyn fungere som deres markedstilsynsmyndighet, unntatt med hensyn til Den europeiske unions domstol når den opptrer innenfor rammen av sin domsmyndighet.

10. Medlemsstatene skal legge til rette for samordning mellom markedstilsynsmyndigheter utpekt i henhold til denne forordningen og andre relevante nasjonale myndigheter eller organer som fører tilsyn med anvendelsen av EU-harmoniseringsregelverk oppført i vedlegg I eller annen unionsrett som kan være relevant for KI-systemene med høy risiko omhandlet i vedlegg III.

11. Markedstilsynsmyndighetene og Kommisjonen skal kunne foreslå felles aktiviteter, herunder felles undersøkelser, som skal utføres enten av markedstilsynsmyndighetene eller av markedstilsynsmyndighetene i fellesskap med Kommisjonen, og som har som mål å fremme samsvar, påvise manglende samsvar, øke bevisstheten om eller gi veiledning om denne forordningen med hensyn til bestemte kategorier av KI-systemer med høy risiko som viser seg å utgjøre en alvorlig risiko i to eller flere medlemsstater, i samsvar med artikkel 9 i forordning (EU) 2019/1020. KI-kontoret skal sørge for samordningsstøtte ved felles undersøkelser.

12. Uten at det berører fullmaktene fastsatt i forordning (EU) 2019/1020, og dersom det er relevant og begrenset til det som er nødvendig for at markedstilsynsmyndighetene skal kunne utføre sine oppgaver, skal leverandørene gi dem full tilgang til den dokumentasjonen og de trenings-, validerings- og testdatasettene som brukes for å utvikle KI-systemer med høy risiko, herunder, dersom det er relevant og omfattet av sikkerhetstiltak, gjennom programmeringsgrensesnitt (API-er) eller andre relevante tekniske midler og verktøy som muliggjør fjerntilgang.

13. Markedstilsynsmyndighetene skal gis tilgang til kildekoden til KI-systemet med høy risiko på begrunnet anmodning og bare når begge følgende vilkår er oppfylt:

- a) Tilgang til kildekoden er nødvendig for å vurdere om et KI-system med høy risiko oppfyller kravene i kapittel III avsnitt 2.
- 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 med fortrolighetsforpliktelsene i artikkel 78.

Artikkel 75

Gjensidig bistand, markedstilsyn og kontroll av KI-systemer for allmenne formål

1. Dersom et KI-system er basert på en KI-modell for allmenne formål, og modellen og systemet er utviklet av samme leverandør, skal KI-kontoret ha fullmakt til å overvåke og føre tilsyn med at det KI-systemet er i samsvar med forpliktelsene etter denne forordningen. For å kunne utføre sine overvåkings- og tilsynsoppgaver skal KI-kontoret ha alle fullmaktene til en markedstilsynsmyndighet slik de er fastsatt i dette avsnittet og i forordning (EU) 2019/1020.

2. Dersom de relevante markedstilsynsmyndighetene har tilstrekkelig grunn til å mene at KI-systemer for allmenne formål som kan brukes direkte av idriftsettere for minst ett formål som er klassifisert som et formål med høy risiko i henhold til denne forordningen, ikke oppfyller kravene fastsatt i denne forordningen, skal de samarbeide med KI-kontoret om å gjennomføre samsvarsvurderinger og skal underrette KI-rådet og andre markedstilsynsmyndigheter om dette.

3. Dersom en markedstilsynsmyndighet ikke er i stand til å fullføre sin undersøkelse av KI-systemet med høy risiko fordi den ikke får tilgang til visse opplysninger om KI-modellen for allmenne formål selv om den har gjort alle rimelige anstrengelser for å innhente disse opplysningene, kan den sende en begrunnet anmodning til KI-kontoret om at det skal håndheve tilgangen til disse opplysningene. I så fall skal KI-kontoret uten ugrunnet opphold, og under alle omstendigheter innen 30 dager, gi den anmodende myndigheten all informasjon som KI-kontoret anser relevant for å fastslå om et KI-system med høy risiko er i samsvar med kravene eller ikke. Markedstilsynsmyndighet skal sikre at opplysningene de innhenter, behandles fortrolig, i samsvar med artikkel 78 i denne forordningen. Prosedyren fastsatt i kapittel VI i forordning (EU) 2019/1020 skal gjelde tilsvarende med nødvendige endringer.

Artikkel 76

Markedstilsynsmyndighetenes tilsyn med testing under virkelige forhold

1. Markedstilsynsmyndighetene skal ha kompetanse og myndighet til å sikre at testing under virkelige forhold skjer i samsvar med denne forordningen.

2. Dersom det utføres testing under virkelige forhold av KI-systemer som det føres tilsyn med innenfor rammen av en regulatorisk sandkasse for KI i henhold til artikkel 58, skal markedstilsynsmyndighetene kontrollere at artikkel 60 overholdes, som et ledd i deres tilsynsrolle for den regulatoriske sandkassen for KI. Disse myndighetene kan, alt etter hva som er relevant, tillate at testingen under virkelige forhold utføres av leverandøren eller den prospektive leverandøren, som unntak fra vilkårene i artikkel 60 nr. 4 bokstav f) og g).

3. Dersom en markedstilsynsmyndighet er blitt informert av den leverandøren, den prospektive leverandøren eller en tredje-part om en alvorlig hendelse, eller har andre grunner til å anta at vilkårene i artikkel 60 og 61 ikke er oppfylt, kan den treffe en av følgende beslutninger på sitt territorium, alt etter hva som er relevant:

- a) Suspendere eller avslutte testingen under virkelige forhold.
- b) Kreve at leverandøren eller den prospektive leverandøren og idriftsetteren eller den prospektive idriftsetteren endrer et hvilket som helst aspekt av testingen under virkelige forhold.

4. Dersom en markedstilsynsmyndighet har truffet en beslutning som nevnt i nr. 3 i denne artikkelen eller har gjort innsigelse i henhold til artikkel 60 nr. 4 bokstav b), skal beslutningen eller innsigelsen inneholde en begrunnelse og angi hvordan leverandøren eller den prospektive leverandøren kan bestride beslutningen eller innsigelsen.

5. Dersom en markedstilsynsmyndighet har truffet en beslutning som nevnt i nr. 3, skal den underrette markedstilsynsmyndighetene i de andre medlemsstatene der KI-systemet er testet i samsvar med testplanen, om dette.

Artikkel 77

Fullmakter for myndigheter som verner grunnleggende rettigheter

1. Nasjonale offentlige myndigheter eller organer som fører tilsyn med eller håndhever overholdelsen av forpliktelsene i henhold til unionsretten om vern av grunnleggende rettigheter, herunder retten til ikke-diskriminering, i forbindelse med bruk av KI-systemer med høy risiko som omhandlet i vedlegg III, skal ha fullmakt til å anmode om og å få tilgang til all dokumentasjon som utarbeides eller vedlikeholdes i henhold til denne forordningen, 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 og offentliggjøre en liste over dem. Medlemsstatene skal underrette Kommisjonen og de øvrige medlemsstatene om listen og holde den oppdatert.

3. Dersom dokumentasjonen nevnt i nr. 1 ikke er tilstrekkelig til å fastslå om en tilsidesettelse av forpliktelsene i henhold til unionsretten om vern av grunnleggende rettigheter har funnet sted, kan den offentlige myndigheten eller det offentlige organet nevnt i nr. 1 framsette en begrunnet anmodning til markedstilsynsmyndigheten om at den organiserer testing av KI-systemet med høy risiko ved hjelp av tekniske midler. Markedstilsynsmyndigheten skal organisere testingen i nært samarbeid med den anmodende offentlige myndigheten eller det anmodende offentlige organet innen rimelig tid etter anmodningen.

4. All informasjon eller dokumentasjon som de nasjonale offentlige myndighetene eller organene nevnt i nr. 1 i denne artikkelen får i samsvar med denne artikkelen, skal behandles i samsvar med fortrolighetsforpliktelsene i artikkel 78.

Artikkel 78

Fortrolighet

1. Kommisjonen, markedstilsynsmyndighetene og de meldte organene samt enhver annen fysisk eller juridisk person som er involvert i anvendelsen av denne forordningen, skal i samsvar med EU-retten eller nasjonal rett respektere fortroligheten av de opplysningene og dataene som innhentes under utførelsen av deres oppgaver og aktiviteter, på en måte som særlig beskytter

- a) en fysisk eller juridisk persons immaterielle rettigheter og fortrolige forretningsinformasjon eller forretningshemmeligheter, herunder kildekode, unntatt i tilfellene nevnt i artikkel 5 i europaparlaments- og rådsdirektiv (EU) 2016/943⁽⁵⁷⁾,
- b) effektiv gjennomføring av denne forordningen, særlig med hensyn til inspeksjoner, undersøkelser eller revisjoner,
- c) offentlige og nasjonale sikkerhetsinteresser,
- d) gjennomføring av straffesaker eller forvaltningssaker,
- e) opplysninger som er gradert i samsvar med unionsretten eller nasjonal rett.

2. Myndighetene som er involvert i anvendelsen av denne forordningen i henhold til nr. 1, skal bare be om opplysninger som er strengt nødvendige for å vurdere risikoen ved KI-systemer og for å utøve deres fullmakter i samsvar med denne forordningen og forordning (EU) 2019/1020. De skal innføre egnede og effektive cybersikkerhetstiltak for å beskytte sikkerheten og fortroligheten til opplysningene og dataene som innhentes, og skal slette de innsamlede dataene 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 på fortrolig grunnlag mellom de nasjonale vedkommende myndighetene eller mellom nasjonale vedkommende myndigheter og Kommisjonen, ikke utleveres uten forutgående samråd med den nasjonale vedkommende myndigheten som opplysningene kommer fra, og idriftsetteren, når KI-systemer med høy risiko som nevnt i nr. 1, 6 eller 7 i vedlegg III brukes av rettshåndhevende myndigheter, grensekontroll-, innvandrings- eller asylmyndigheter, og når slik utlevering vil sette offentlige og nasjonale sikkerhetsinteresser i fare. Denne utvekslingen av opplysninger skal ikke omfatte sensitive operasjonelle data om virksomheten til rettshåndhevende myndigheter, grensekontroll-, innvandrings- eller asylmyndigheter.

Når de rettshåndhevende myndighetene, innvandrings- eller asylmyndighetene er leverandører av KI-systemer med høy risiko som omhandlet i nr. 1, 6 eller 7 i vedlegg III, skal den tekniske dokumentasjonen omhandlet i vedlegg IV oppbevares i nevnte myndigheters lokaler. Nevnte myndigheter skal sikre at markedstilsynsmyndighetene omhandlet 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 personale hos markedstilsynsmyndigheten som har det tilstrekkelige nivået av sikkerhetsklarering, skal ha tilgang til denne dokumentasjonen eller enhver kopi av den.

4. Nr. 1 og 3 berører ikke rettighetene og forpliktelsene til Kommisjonen, medlemsstatene og deres relevante myndigheter samt meldte organer når det gjelder utveksling av informasjon og offentliggjøring av advarsler, herunder i sammenheng med samarbeid over landegrensene, og heller ikke de berørte partenes plikt til å utlevere informasjon i henhold til strafferetten i medlemsstatene.

5. Kommisjonen og medlemsstatene kan, dersom det er nødvendig og forenlig med relevante bestemmelser i internasjonale avtaler og handelsavtaler, utveksle fortrolig informasjon med reguleringsmyndigheter i tredjeland som de har inngått bilaterale eller multilaterale fortrolighetsavtaler med som sikrer et tilstrekkelig fortrolighetsnivå.

Artikkel 79

Prosedyre på nasjonalt plan for å håndtere KI-systemer som utgjør en risiko

1. KI-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, 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 artikkelen, skal den foreta en vurdering av det aktuelle KI-systemet med hensyn til dets samsvar med alle kravene og forpliktelsene fastsatt i denne forordningen. Det skal legges særlig vekt på KI-systemer som utgjør en risiko for sårbare grupper. Dersom det avdekkes risiko for grunnleggende rettigheter, skal markedstilsynsmyndigheten også informere og samarbeide fullt ut med de relevante nasjonale offentlige myndighetene eller organene nevnt i artikkel 77 nr. 1. De relevante operatørene skal ved behov 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 beskyttelse av fortrolig knowhow og fortrolige forretningsopplysninger (forretningshemmeligheter) mot ulovlig tilegnelse, bruk og formidling (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, ved denne vurderingen finner at KI-systemet ikke er i samsvar med kravene og forpliktelsene fastsatt i denne forordningen, skal den uten ugrunnet opphold kreve at den relevante operatøren treffer alle egnede korrigerende tiltak for å bringe KI-systemet i samsvar, for å trekke det tilbake fra markedet eller for å tilbakekalle det innen en frist som markedstilsynsmyndigheten kan fastsette, og under alle omstendigheter innen 15 virkedager, eller innen en frist fastsatt i det relevante EU-harmoniseringsregelverket, avhengig av hvilken frist som er kortest.

Markedstilsynsmyndigheten skal underrette det relevante meldte organet om dette. Artikkel 18 i forordning (EF) nr. 2019/1020 får anvendelse på tiltakene nevnt i andre ledd i dette nummeret.

3. Dersom markedstilsynsmyndigheten finner at det manglende samsvaret ikke er begrenset til dens nasjonale territorium, skal den uten ugrunnet opphold underrette Kommisjonen og de andre medlemsstatene om resultatene av vurderingen og om de tiltakene den har pålagt operatøren å treffe.

4. Operatøren skal sikre at alle egnede korrigerende tiltak blir truffet med hensyn til alle de aktuelle KI-systemene som den har gjort tilgjengelig på unionsmarkedet.

5. Dersom en operatør av et KI-system ikke treffer egnede korrigerende tiltak innen fristen nevnt i nr. 2 andre ledd, skal markedstilsynsmyndigheten treffe alle egnede midlertidige tiltak for å forby at KI-systemet gjøres tilgjengelig på det nasjonale markedet eller begrense slik tilgjengeliggjøring, eller for å trekke produktet eller det frittstående KI-systemet tilbake fra dette markedet eller tilbakekalle det. Nevnte myndighet skal uten ugrunnet opphold underrette Kommisjonen og de andre medlemsstatene om disse tiltakene.

6. Underretningen nevnt i nr. 5 skal omfatte alle tilgjengelige opplysninger, særlig de opplysningene som er nødvendige for å identifisere det ikke-samsvarende KI-systemet, KI-systemets opprinnelse, det påståtte manglende samsvarets art og risikoen som er involvert, arten og varigheten av de nasjonale tiltakene som er truffet, og argumentene framsatt av den relevante operatøren. Markedstilsynsmyndighetene skal særlig angi om det manglende samsvaret har en eller flere av følgende årsaker:

- a) Manglende overholdelse av forbudet mot de formene for KI-praksis som er omhandlet i artikkel 5.
- b) At et KI-system med høy risiko ikke oppfyller kravene i kapittel III avsnitt 2.
- c) Mangler ved de harmoniserte standardene eller felles spesifikasjonene omhandlet i artikkel 40 og 41 som gir formodning om samsvar.
- d) Manglende overholdelse av artikkel 50.

7. Markedstilsynsmyndighetene utenom markedstilsynsmyndigheten i den medlemsstaten som har innledet prosedyren, skal uten ugrunnet opphold underrette Kommisjonen og de andre medlemsstatene om eventuelle tiltak som er truffet, og eventuelle tilleggsopplysninger de har om det aktuelle KI-systemets manglende samsvar, samt, dersom de er uenige i det meldte nasjonale tiltaket, om sine innsigelser.

8. Dersom det innen tre måneder etter at underretningen nevnt i nr. 5 i denne artikkelen er mottatt, verken er reist innsigelser av en markedstilsynsmyndighet i en medlemsstat eller av Kommisjonen mot et midlertidig tiltak truffet av en medlemsstat, skal tiltaket anses for å være berettiget. Dette berører ikke den aktuelle operatørens prosessuelle rettigheter i samsvar med artikkel 18 i forordning (EU) 2019/1020. Tremånedersperioden nevnt i dette nummeret skal reduseres til 30 dager ved manglende overholdelse av forbudet mot de formene for KI-praksis som er omhandlet i artikkel 5 i denne forordningen.

9. Markedstilsynsmyndighetene skal sikre at det uten ugrunnet opphold treffes egnede begrensende tiltak med hensyn til det aktuelle produktet eller KI-systemet, for eksempel at produktet eller KI-systemet trekkes tilbake fra deres marked.

Artikkel 80

Prosedyre for håndtering av KI-systemer som leverandøren har klassifisert som uten høy risiko, ved anvendelse av vedlegg III

1. Dersom en markedstilsynsmyndighet har tilstrekkelig grunn til å mene at et KI-system som leverandøren har klassifisert som et KI-system uten høy risiko i samsvar med artikkel 6 nr. 3, faktisk er et KI-system med høy risiko, skal markedstilsynsmyndigheten foreta en vurdering av det aktuelle KI-systemet med hensyn til dets klassifisering som et KI-system med høy risiko, basert på vilkårene i artikkel 6 nr. 3 og Kommisjonens retningslinjer.

2. Dersom markedstilsynsmyndigheten ved denne vurderingen finner at det aktuelle KI-systemet er et KI-system med høy risiko, skal den uten ugrunnet opphold kreve at den relevante leverandøren treffer alle nødvendige tiltak for å bringe KI-systemet i samsvar med kravene og forpliktelsene fastsatt i denne forordningen og treffer egnede korrigerende tiltak innen en frist som markedstilsynsmyndigheten kan fastsette.
3. Dersom markedstilsynsmyndigheten finner at bruken av det aktuelle KI-systemet ikke er begrenset til dens nasjonale territorium, skal den uten ugrunnet opphold underrette Kommisjonen og de andre medlemsstatene om resultatene av vurderingen og om de tiltakene den har pålagt leverandøren å treffe.
4. Leverandøren skal sikre at alle nødvendige tiltak treffes for å bringe KI-systemet i samsvar med kravene og forpliktelsene fastsatt i denne forordningen. Dersom leverandøren av et slikt KI-system ikke bringer KI-systemet i samsvar med disse kravene og forpliktelsene innen fristen nevnt i nr. 2 i denne artikkelen, skal leverandøren ilegges overtredelsesgebyrer i samsvar med artikkel 99.
5. Leverandøren skal sikre at alle egnede korrigerende tiltak blir truffet med hensyn til alle de aktuelle KI-systemene som den har gjort tilgjengelig på unionsmarkedet.
6. Dersom leverandøren av det aktuelle KI-systemet ikke treffer egnede korrigerende tiltak innen fristen nevnt i nr. 2 i denne artikkelen, får artikkel 79 nr. 5–9 anvendelse.
7. Dersom markedstilsynsmyndigheten ved vurderingen i henhold til nr. 1 i denne artikkel fastslår at KI-systemet er feilklassifisert av leverandøren som et system uten høy risiko for å omgå anvendelsen av kravene i kapittel III avsnitt 2, skal leverandøren ilegges overtredelsesgebyrer i samsvar med artikkel 99.
8. Når de utøver sin myndighet til å overvåke anvendelsen av denne artikkelen, og i samsvar med artikkel 11 i forordning (EU) 2019/1020, kan markedstilsynsmyndighetene gjennomføre egnede kontroller der de særlig tar i betraktning opplysninger som er lagret i EU-databasen omhandlet i artikkel 71 i denne forordningen.

Artikkel 81

EU-beskyttelsesprosedyre

1. Dersom det innen tre måneder etter mottak av underretningen nevnt i artikkel 79 nr. 5, eller innen 30 dager ved manglende overholdelse av forbudet mot de formene for KI-praksis som er omhandlet i artikkel 5, reises innsigelser fra markedstilsynsmyndigheten i en medlemsstat mot et tiltak truffet av en annen markedstilsynsmyndighet, eller dersom Kommisjonen anser at tiltaket strider mot unionsretten, skal Kommisjonen uten ugrunnet opphold innlede samråd med markedstilsynsmyndigheten i den relevante medlemsstaten og med operatøren eller operatørene og evaluere det nasjonale tiltaket. På grunnlag av resultatene av denne evalueringen skal Kommisjonen innen seks måneder, eller innen 60 dager ved manglende overholdelse av forbudet mot de formene for KI-praksis som er omhandlet i artikkel 5, regnet fra meldingen nevnt i artikkel 79 nr. 5, avgjøre om det nasjonale tiltaket er berettiget, og underrette markedstilsynsmyndigheten i den aktuelle medlemsstaten om sin avgjørelse. Kommisjonen skal også underrette alle de andre markedstilsynsmyndighetene om sin avgjørelse.
2. Dersom Kommisjonen finner at tiltaket som den relevante medlemsstaten har truffet, er berettiget, skal alle medlemsstater sikre at de treffer egnede begrensende tiltak med hensyn til det aktuelle KI-systemet, for eksempel kreve at KI-systemet trekkes tilbake fra deres marked uten ugrunnet opphold, og skal underrette Kommisjonen om dette. Dersom Kommisjonen finner at det nasjonale tiltaket ikke er berettiget, skal medlemsstaten det gjelder, trekke det tilbake og underrette Kommisjonen om dette.
3. Dersom det nasjonale tiltaket anses som berettiget, og KI-systemets manglende samsvar tilskrives mangler ved de harmoniserte standardene omhandlet i artikkel 40 og 41 i denne forordningen, skal Kommisjonen anvende prosedyren fastsatt i artikkel 11 i forordning (EU) nr. 1025/2012.

Artikkel 82

Samsvarende KI-systemer som utgjør en risiko

1. Dersom markedstilsynsmyndigheten i en medlemsstat etter å ha foretatt en vurdering i samsvar med artikkel 79 og etter å ha rådført seg med den relevante nasjonale offentlige myndigheten nevnt i artikkel 77 nr. 1 fastslår at et KI-system med høy risiko som, selv om det er i samsvar med denne forordningen, likevel utgjør en risiko for menneskers helse eller sikkerhet, for grunnleggende rettigheter eller for andre aspekter av vernet av allmenne interesser, skal den kreve at den relevante operatøren uten ugrunnet opphold og innen en frist som markedstilsynsmyndigheten kan fastsette, treffer alle egnede tiltak for å sikre at KI-systemet det gjelder, ikke lenger utgjør nevnte risiko når det bringes i omsetning eller tas i bruk.

2. Leverandøren eller en annen relevant operatør skal sikre at det treffes korrigerende tiltak med hensyn til alle aktuelle KI-systemer som denne har gjort tilgjengelig på unionsmarkedet, innen fristen som er fastsatt av markedstilsynsmyndigheten i medlemsstaten nevnt i nr. 1.
3. Medlemsstatene skal umiddelbart underrette Kommisjonen og de andre medlemsstatene om en konklusjon i henhold til nr. 1. Denne underretningen skal inneholde alle tilgjengelige opplysninger, særlig de dataene som er nødvendige for å identifisere det aktuelle KI-systemet, KI-systemets opprinnelse og omsetningskjede, arten av den risikoen som er involvert, og arten og varigheten av de nasjonale tiltakene som er truffet.
4. Kommisjonen skal uten ugrunnet opphold innlede samråd med medlemsstatene det gjelder, og de relevante operatørene og skal evaluere det nasjonale tiltaket som er truffet. På grunnlag av resultatene av denne evalueringen skal Kommisjonen avgjøre om tiltaket er berettiget eller ikke, og om nødvendig foreslå andre egnede tiltak.
5. Kommisjonen skal umiddelbart meddele sin avgjørelse til medlemsstatene det gjelder, og de relevante operatørene. Den skal også underrette de øvrige medlemsstatene.

Artikkel 83

Formelt manglende samsvar

1. Dersom markedstilsynsmyndigheten i en medlemsstat konstaterer ett av følgende, skal den pålegge den aktuelle leverandøren å bringe det manglende samsvaret til opphør:
 - a) CE-merkingen er påført i strid med artikkel 48.
 - b) CE-merkingen er ikke påført.
 - c) EU-samsvarserklæringen omhandlet i artikkel 47 er ikke utarbeidet.
 - d) EU-samsvarserklæringen omhandlet i artikkel 47 er ikke utarbeidet på riktig måte.
 - e) Registrering i EU-databasen omhandlet i artikkel 71 er ikke gjennomført.
 - f) Det er ikke utpekt en bemyndiget representant, dersom dette er relevant.
 - g) Teknisk dokumentasjon er ikke tilgjengelig.
2. Dersom det manglende samsvaret omhandlet i nr. 1 vedvarer, skal markedstilsynsmyndigheten i medlemsstaten det gjelder, treffe egnede tiltak for å begrense eller forby at KI-systemet med høy risiko gjøres tilgjengelig på markedet, eller sikre at det uten ugrunnet opphold tilbakekalles eller trekkes tilbake.

Artikkel 84

EU-støttestrukturer for KI-testing

1. Kommisjonen skal utpeke en eller flere EU-støttestrukturer for KI-testing til å utføre oppgavene nevnt i artikkel 21 nr. 6 i forordning (EU) 2019/1020 på KI-området.
2. Uten at det berører oppgavene nevnt i nr. 1, skal EU-støttestrukturer for KI-testing også yte teknisk eller vitenskapelig rådgivning på anmodning fra KI-rådet, Kommisjonen eller markedstilsynsmyndighetene.

AVSNITT 4

Rettsmidler

Artikkel 85

Rett til å klage til en markedstilsynsmyndighet

Uten at det berører annen forvaltningsmessig klageadgang eller andre rettsmidler, kan enhver fysisk eller juridisk person som har grunn til å anta at det foreligger en overtredelse av bestemmelsene i denne forordningen, inngi klager til den relevante markedstilsynsmyndigheten.

I samsvar med forordning (EU) 2019/1020 skal det tas hensyn til slike klager med henblikk på å gjennomføre markedstilsynsaktiviteter, og de skal behandles i samsvar med de særskilte prosedyrene som markedstilsynsmyndighetene har fastsatt for dem.

Artikkel 86

Rett til forklaring på individuelle beslutninger

1. Enhver person som blir berørt av en beslutning som idriftsetteren treffer på grunnlag av utdata fra et KI-system med høy risiko oppført i vedlegg III, med unntak av systemer oppført i nr. 2 i nevnte vedlegg, og som har rettsvirkninger eller på lignende måte i betydelig grad påvirker personen på en måte som vedkommende anser for å ha negativ innvirkning på personens helse, sikkerhet eller grunnleggende rettigheter, skal ha rett til å få en klar og meningsfull forklaring på KI-systemets rolle i beslutningsprosessen og de viktigste elementene i beslutningen som treffes.

2. Nr. 1 får ikke anvendelse på bruk av KI-systemer som omfattes av unntak fra eller begrensninger av forpliktelsen i henhold til nevnte nummer som følger av unionsretten eller av nasjonal rett i samsvar med unionsretten.

3. Denne artikkel får anvendelse bare i den utstrekning retten nevnt i nr. 1 ikke på annen måte er fastsatt i unionsretten.

Artikkel 87

Rapportering av overtredelser og beskyttelse av personer som rapporterer

Direktiv (EU) 2019/1937 får anvendelse på rapportering av alle overtredelser av denne forordningen og på beskyttelse av personer som rapporterer slike overtredelser.

AVSNITT 5

Tilsyn, undersøkelse, håndhevelse og overvåking med hensyn til leverandører av KI-modeller for allmenne formål

Artikkel 88

Håndhevelse av forpliktelsene til leverandører av KI-modeller for allmenne formål

1. Kommisjonen skal ha enekompetanse til å føre tilsyn med og håndheve kapittel V, idet det tas hensyn til garantiene for rett saksbehandling i henhold til artikkel 94. Kommisjonen skal overlate gjennomføringen av disse oppgavene til KI-kontoret, uten at det berører Kommisjonens organisasjonsrett og kompetansefordelingen mellom medlemsstatene og Unionen på grunnlag av traktatene.

2. Uten at det berører artikkel 75 nr. 3, kan markedstilsynsmyndighetene anmode Kommisjonen om å utøve fullmaktene fastsatt i dette avsnittet dersom det er nødvendig og forholdsmessig for å bistå dem med å utføre sine oppgaver i henhold til denne forordningen.

*Artikkel 89***Overvåkingstiltak**

1. For å utføre de oppgavene som tildeles det i henhold til dette avsnittet, kan KI-kontoret treffe de nødvendige tiltakene for å overvåke at leverandører av KI-modeller for allmenne formål gjennomfører og overholder denne forordningen på en effektiv måte, herunder at de overholder de godkjente reglene for god praksis.
2. Nedstrømsleverandører skal ha rett til å klage på en overtredelse av denne forordningen. En klage skal være behørig begrunnet og inneholde minst følgende informasjon:
 - a) Kontaktpunktet for leverandøren av den aktuelle KI-modellen for allmenne formål.
 - b) En beskrivelse av de relevante faktiske forholdene, de aktuelle bestemmelsene i denne forordningen og grunnen til at nedstrømsleverandøren anser at leverandøren av den aktuelle KI-modellen for allmenne formål har overtrådt denne forordningen.
 - c) All annen informasjon som anses som relevant av nedstrømsleverandøren som har sendt anmodningen, herunder, dersom det er relevant, informasjon som nedstrømsleverandøren har innhentet på eget initiativ.

*Artikkel 90***Varsler om systemrisiko fra vitenskapspanelet**

1. Vitenskapspanelet kan sende et kvalifisert varsel til KI-kontoret dersom det har grunn til å mistenke at
 - a) en KI-modell for allmenne formål utgjør en konkret identifiserbar risiko på unionsplan, eller
 - b) en KI-modell for allmenne formål oppfyller vilkårene nevnt i artikkel 51.
2. Etter et slikt kvalifisert varsel kan Kommisjonen, gjennom KI-kontoret og etter å ha underrettet KI-rådet, utøve fullmakten fastsatt i dette avsnittet for å vurdere saken. KI-kontoret skal underrette KI-rådet om ethvert tiltak i henhold til artikkel 91–94.
3. Et kvalifisert varsel skal være behørig begrunnet og inneholde minst følgende informasjon:
 - a) Kontaktpunktet for leverandøren av den aktuelle KI-modellen for allmenne formål med systemrisiko.
 - b) En beskrivelse av de relevante faktiske forholdene og grunnene til varselet fra vitenskapspanelet.
 - c) Eventuell annen informasjon som vitenskapspanelet anser som relevant, herunder, dersom det er relevant, informasjon som det har innhentet på eget initiativ.

*Artikkel 91***Fullmakt til å anmode om dokumentasjon og informasjon**

1. Kommisjonen kan anmode leverandøren av den aktuelle KI-modellen for allmenne formål om å framlegge den dokumentasjonen som leverandøren har utarbeidet i samsvar med artikkel 53 og 55, eller eventuell ytterligere informasjon som er nødvendig for å vurdere om leverandøren overholder denne forordningen.
2. Før anmodningen om informasjon sendes, kan KI-kontoret innlede en strukturert dialog med leverandøren av KI-modellen for allmenne formål.
3. Etter en behørig begrunnet anmodning fra vitenskapspanelet kan Kommisjonen utstede en anmodning om informasjon til en leverandør av en KI-modell for allmenne formål dersom tilgang til informasjonen er nødvendig og forholdsmessig for at vitenskapspanelet skal kunne utføre sine oppgaver i henhold til artikkel 68 nr. 2.

4. Anmodningen om informasjon skal angi det rettslige grunnlaget for og formålet med anmodningen, hvilken informasjon det anmodes om, fristen for å gi informasjonen og de overtredelsesgebyrene som er fastsatt i artikkel 101 for å gi uriktig, ufullstendig eller villedende informasjon.

5. Leverandøren av den aktuelle KI-modellen for allmenne formål eller dennes representant skal gi den informasjonen det anmodes om. Dersom det dreier seg om juridiske personer, selskaper eller firmaer, eller dersom leverandøren ikke har status som juridisk person, skal de personene som i henhold til lov eller vedtekter har fullmakt til å representere dem, gi informasjonen det anmodes om, på vegne av leverandøren av den aktuelle KI-modellen for allmenne formål. Advokater med behørig fullmakt kan gi informasjonen på vegne av sine klienter. Klientene bærer likevel det fulle ansvaret dersom informasjonen som gis, er ufullstendig, uriktig eller villedende.

Artikkel 92

Fullmakt til å gjennomføre evalueringer

1. KI-kontoret kan etter samråd med KI-rådet gjennomføre evalueringer av den aktuelle KI-modellen for allmenne formål for å

- a) vurdere om leverandøren overholder forpliktelsene i henhold til denne forordningen, dersom informasjonen som er innhentet i samsvar med artikkel 91, er tilstrekkelig, eller
- b) undersøke systemrisikoen på unionsplan i KI-modeller for allmenne formål med systemrisiko, særlig etter et kvalifisert varsel fra vitenskapspanelet i samsvar med artikkel 90 nr. 1 bokstav a).

2. Kommisjonen kan beslutte å utpeke uavhengige eksperter til å gjennomføre evalueringer på Kommisjonens vegne, herunder fra vitenskapspanelet nedsatt i samsvar med artikkel 68. Uavhengige eksperter som utpekes til denne oppgaven, skal oppfylle kriteriene i artikkel 68 nr. 2.

3. Ved anvendelsen av nr. 1 kan Kommisjonen anmode om tilgang til den aktuelle KI-modellen for allmenne formål gjennom API-er eller andre egnede tekniske midler og verktøy, herunder kildekode.

4. Anmodningen om tilgang skal angi det rettslige grunnlaget for, formålet med og grunnene til anmodningen, fristen for å gi tilgang og de overtredelsesgebyrene som er fastsatt i artikkel 101 for å unnlate å gi tilgang.

5. Leverandøren av den aktuelle KI-modellen for allmenne formål eller dennes representant skal gi den informasjonen det anmodes om. Dersom det dreier seg om juridiske personer, selskaper eller firmaer, eller dersom leverandøren ikke har status som juridisk person, skal de personene som i henhold til lov eller vedtekter har fullmakt til å representere dem, gi den tilgangen det anmodes om, på vegne av leverandøren av den aktuelle KI-modellen for allmenne formål.

6. Kommisjonen skal vedta gjennomføringsrettsakter som fastsetter de nærmere ordningene og vilkårene for evalueringene, herunder de nærmere ordningene for å involvere uavhengige eksperter og prosedyren for å velge dem ut. Disse gjennomføringsrettsaktene skal vedtas i samsvar med undersøkelsesprosedyren nevnt i artikkel 98 nr. 2.

7. Før KI-kontoret anmoder om tilgang til den aktuelle KI-modellen for allmenne formål, kan det innlede en strukturert dialog med leverandøren av KI-modellen for allmenne formål for å innhente mer informasjon om den interne testingen av modellen, de interne sikkerhetstiltakene for å forebygge systemrisiko og andre interne prosedyrer og tiltak som leverandøren har iverksatt for å begrense slik risiko.

Artikkel 93

Fullmakt til å anmode om tiltak

1. Dersom det er nødvendig og hensiktsmessig, kan Kommisjonen anmode leverandører om å

- a) treffe egnede tiltak for å overholde forpliktelsene fastsatt i artikkel 53 og 54,

- b) treffe avbøtende tiltak dersom evalueringen som er gjennomført i samsvar med artikkel 92, har gitt opphav til alvorlig og begrunnet mistanke om en systemrisiko på unionsplan,
 - c) begrense tilgjengeliggjøring av modellen på markedet, trekke den tilbake eller tilbakekalle den.
2. Før det anmodes om et tiltak, kan KI-kontoret innlede en strukturert dialog med leverandøren av KI-modellen for allmenne formål.
3. Dersom leverandøren av KI-modellen for allmenne formål med systemrisiko i løpet av den strukturerte dialogen nevnt i nr. 2 gir tilsagn om å gjennomføre avbøtende tiltak for å håndtere en systemrisiko på unionsplan, kan Kommisjonen ved en beslutning gjøre disse tilsagnene bindende og erklære at det ikke er ytterligere grunnlag for tiltak.

Artikkel 94

Prosessuelle rettigheter for markedsdeltakere i forbindelse med KI-modellen for allmenne formål

Artikkel 18 i forordning (EU) 2019/1020 skal gjelde tilsvarende med nødvendige endringer for leverandørene av KI-modellen for allmenne formål, uten at det berører mer spesifikke prosessuelle rettigheter fastsatt i denne forordningen.

KAPITTEL X

ATFERDSREGLER OG RETNINGSLINJER

Artikkel 95

Atferdsregler for frivillig anvendelse av særlige krav

1. KI-kontoret og medlemsstatene skal oppmuntre til og lette utarbeiding av atferdsregler, herunder tilhørende forvaltningsmekanismer, som har til hensikt å fremme frivillig anvendelse av noen av eller alle kravene i vedlegg III avsnitt 2 på KI-systemer, unntatt KI-systemer med høy risiko, idet det tas hensyn til de tilgjengelige tekniske løsningene og bransjens beste praksis som gjør det mulig å anvende slike krav.
2. KI-kontoret og medlemsstatene skal lette utarbeiding av atferdsregler om frivillig anvendelse av særlige krav på alle KI-systemer, herunder fra idriftsetters side, basert på klare mål og nøkkeltallsindikatorer for å måle oppnåelsen av disse målene, herunder, men ikke begrenset til
 - a) relevante elementer fastsatt i Unionens etiske retningslinjer for pålitelig KI,
 - b) å vurdere og å minimere innvirkningen av KI-systemer på miljømessig bærekraft, også når det gjelder energieffektiv programmering og teknikker for effektiv utforming, trening og bruk av KI,
 - c) å fremme KI-kompetanse, særlig hos personer som arbeider med utvikling, drift og bruk av KI,
 - d) å lette en inkluderende og mangfoldig utforming av KI-systemer, herunder gjennom etablering av inkluderende og mangfoldige utviklingsteam og ved å stimulere til at berørte parter deltar i denne prosessen,
 - e) å vurdere og å forebygge den negative innvirkningen av KI-systemer på sårbare personer eller grupper av sårbare personer, også når det gjelder tilgjengelighet for personer med nedsatt funksjonsevne, og på likestillingen mellom kjønnene.
3. Atferdsregler kan utarbeides av individuelle leverandører eller idriftsettere av KI-systemer eller av organisasjoner som representerer dem, eller av begge, herunder med medvirkning av alle berørte parter og deres representative organisasjoner, herunder sivilsamfunnsorganisasjoner og akademia. Atferdsregler kan omfatte ett eller flere KI-systemer, tatt i betraktning likheten mellom de relevante systemenes tiltenkte formål.
4. KI-kontoret og medlemsstatene skal ta hensyn til de særskilte interessene og behovene til små og mellomstore bedrifter, herunder oppstartsbedrifter, når de oppmuntrer til og legger til rette for utarbeiding av atferdsregler.

Artikkel 96

Retningslinjer fra Kommisjonen for gjennomføring av denne forordningen

1. Kommisjonen skal utarbeide retningslinjer for den praktiske gjennomføringen av denne forordningen, særlig når det gjelder
 - a) anvendelsen av kravene og forpliktelsene omhandlet i artikkel 8–15 og artikkel 25,
 - b) den forbudte praksisen omhandlet i artikkel 5,
 - c) den praktiske gjennomføringen av bestemmelsene om vesentlige endringer,
 - d) den praktiske gjennomføringen av forpliktelsene om åpenhet fastsatt i artikkel 50,
 - e) detaljert informasjon om denne forordningens forhold til EU-harmoniseringsregelverket oppført i vedlegg I og til annen relevant unionsrett, også når det gjelder konsekvens i håndhevelsen av regelverket,
 - f) anvendelsen av definisjonen av et KI-system i artikkel 3 nr. 1.

Når Kommisjonen utsteder slike retningslinjer, skal den ta særlig hensyn til behovene til små og mellomstore bedrifter, herunder oppstartsbedrifter, samt behovene til lokale offentlige myndigheter og de sektorene som mest sannsynlig vil bli berørt av denne forordningen.

Retningslinjene nevnt i første ledd i dette nummeret skal ta behørig hensyn til det allment anerkjente aktuelle tekniske utviklingstrinnet for KI, samt til relevante harmoniserte standarder og felles spesifikasjoner som omhandlet i artikkel 40 og 41, eller til de harmoniserte standardene eller tekniske spesifikasjonene som er fastsatt i samsvar med EU-harmoniseringsregelverket.

2. På anmodning fra medlemsstatene eller KI-kontoret eller på eget initiativ skal Kommisjonen oppdatere tidligere vedtatte retningslinjer når det anses nødvendig.

KAPITTEL XI

DELEGERING AV MYNDIGHET OG KOMITÉPROSEDYRE

Artikkel 97

Utøvelse av delegert myndighet

1. Myndigheten til å vedta delegerte rettsakter gis Kommisjonen på vilkårene fastsatt i denne artikkelen.
2. Myndigheten til å vedta delegerte rettsakter 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 gis Kommisjonen for en periode på fem år fra 1. august 2024. Kommisjonen skal utarbeide en rapport om den delegerte myndigheten senest ni måneder før utgangen av femårsperioden. Den delegerte myndigheten skal stilltiende forlenges med perioder av samme varighet med mindre Europaparlamentet eller Rådet motsetter seg slik forlengelse senest tre måneder før utgangen av hver periode.
3. Den delegerte myndigheten 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 Europaparlamentet eller Rådet. En beslutning om tilbakekalling innebærer at den delegerte myndigheten som angis i beslutningen, opphører å gjelde. Tilbakekallingen trer i kraft dagen etter at den er kunngjort i *Den europeiske unions tidende*, eller på et senere tidspunkt som er angitt i beslutningen. Den berører ikke gyldigheten av delegerte rettsakter som allerede er trådt i kraft.
4. Før Kommisjonen vedtar en delegert rettsakt, skal den rådspørre eksperter utpekt av hver medlemsstat i samsvar med prinsippene fastsatt i den tverrinstitusjonelle avtalen av 13. april 2016 om bedre regelverksutforming.

5. Så snart Kommisjonen vedtar en delegert rettsakt, skal den underrette Europaparlamentet og Rådet samtidig om dette.
6. En 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 trer i kraft bare dersom verken Europaparlamentet eller Rådet har gjort innsigelse innen en frist på tre måneder etter at rettsakten ble meddelt Europaparlamentet og Rådet, eller dersom både Europaparlamentet og Rådet innen utløpet av denne fristen har underrettet Kommisjonen om at de ikke har til hensikt å gjøre innsigelse. På Europaparlamentets eller Rådets initiativ forlenges denne fristen med tre måneder.

Artikkel 98

Komitéprosedyre

1. Kommisjonen skal bistås av en komité. Nevnte komité skal være en komité i samsvar med forordning (EU) nr. 182/2011.
2. Når det vises til dette nummeret, får artikkel 5 i forordning (EU) nr. 182/2011 anvendelse.

KAPITTEL XII

SANKSJONER

Artikkel 99

Sanksjoner

1. I samsvar med vilkårene fastsatt i denne forordningen skal medlemsstatene fastsette regler for sanksjoner og andre håndhevels tiltak, som også kan omfatte advarsler og ikke-monetære tiltak, som får anvendelse ved operatørs overtredelse av denne forordningen, og treffe alle nødvendige tiltak for å sikre at sanksjonene gjennomføres på en forsvarlig og effektiv måte, idet det tas hensyn til retningslinjene utstedt av Kommisjonen i henhold til artikkel 96. De fastsatte sanksjonene skal være virkningsfulle, stå i forhold til overtredelsen og virke avskrekkende. De skal ta hensyn til interessene til små og mellomstore bedrifter, herunder oppstartsbedrifter, og deres økonomiske levedyktighet.
2. Medlemsstatene skal uten ugrunnet opphold og senest på ikrafttredelsesdatoen underrette Kommisjonen om reglene for sanksjoner og andre håndhevels tiltak som nevnt i nr. 1 og uten ugrunnet opphold underrette den om eventuelle senere endringer av dem.
3. Ved manglende overholdelse av forbudet mot de formene for KI-praksis som er omhandlet i artikkel 5, skal det ilegges overtredelsesgebyrer på opptil 35 000 000 euro eller, dersom overtredelsen begås av et foretak, opptil 7 % av dets samlede globale årsomsetning i det foregående regnskapsåret, avhengig av hvilket beløp som er høyest.
4. Ved manglende overholdelse av følgende bestemmelser som gjelder operatører eller meldte organer, utover dem som er fastsatt i artikkel 5, skal det ilegges overtredelsesgebyrer på opptil 15 000 000 euro eller, dersom overtredelsen begås av et foretak, opptil 3 % av dets samlede globale årsomsetning i det foregående regnskapsåret, avhengig av hvilket beløp som er høyest:
 - a) Forpliktelsene for leverandører i henhold til artikkel 16.
 - b) Forpliktelsene for bemyndigede representanter i henhold til artikkel 22.
 - c) Forpliktelsene for importører i henhold til artikkel 23.
 - d) Forpliktelsene for distributører i henhold til artikkel 24.
 - e) Forpliktelsene for idriftsettere i henhold til artikkel 26.
 - f) Kravene til og forpliktelsene for meldte organer i henhold til artikkel 31, artikkel 33 nr. 1, 3 og 4 eller artikkel 34.
 - g) Åpenhetsforpliktelsene for leverandører og idriftsettere i henhold til artikkel 50.

5. Ved utlevering av uriktig, ufullstendig eller villedende informasjon til meldte organer eller nasjonale vedkommende myndigheter som svar på en anmodning skal det ilegges overtredelsesgebyrer på opptil 7 500 000 euro eller, dersom overtredelsen begås av et foretak, opptil 1 % av dets samlede globale årsomsetning i det foregående regnskapsåret, avhengig av hvilket beløp som er høyest.
6. For små og mellomstore bedrifter, herunder oppstartsbedrifter, skal hvert overtredelsesgebyr nevnt i denne artikkelen være på opptil den prosentandelen eller det beløpet som er nevnt i nr. 3, 4 og 5, avhengig av hvilket beløp som er lavest.
7. Når det treffes beslutning om hvorvidt det skal ilegges et overtredelsesgebyr, og om overtredelsesgebyrets størrelse i hvert enkelt tilfelle, skal alle relevante omstendigheter i den spesifikke situasjonen tas i betraktning, og alt etter hva som er relevant, skal det tas hensyn til følgende:
 - a) Karakteren, alvorlighetsgraden og varigheten av overtredelsen og av dens konsekvenser, tatt i betraktning KI-systemets formål og, dersom det er relevant, antallet berørte personer og omfanget av den skaden de har lidd.
 - b) Om andre markedstilsynsmyndigheter allerede har ilagt den samme operatøren overtredelsesgebyrer for samme overtredelse.
 - c) Om andre myndigheter allerede har ilagt den samme operatøren overtredelsesgebyrer for overtredelse av annen unionsrett eller nasjonal rett, når disse overtredelsene skyldes den samme aktiviteten eller unnlatelsen som utgjør en relevant overtredelse av denne forordningen.
 - d) Størrelsen på samt årsomsetningen og markedsandelen til operatøren som har begått overtredelsen.
 - e) Enhver annen skjerpene eller formildende faktor ved sakens omstendigheter, for eksempel økonomiske fordeler som er oppnådd, eller tap som er unngått, direkte eller indirekte, som følge av overtredelsen.
 - f) Graden av samarbeid med de nasjonale vedkommende myndighetene for å bøte på overtredelsen og redusere de mulige negative virkningene av den.
 - g) Graden av ansvar hos operatøren, tatt i betraktning de tekniske og organisatoriske tiltakene som operatøren har iverksatt.
 - h) På hvilken måte de nasjonale vedkommende myndighetene har fått kjennskap til overtredelsen, særlig om og i så fall i hvilken grad operatøren har underrettet om den.
 - i) Om overtredelsen er begått forsettlig eller uaktsomt.
 - j) Eventuelle tiltak som operatøren har truffet for å begrense skaden som de berørte personene har lidd.
8. Hver medlemsstat skal fastsette regler om i hvilken grad offentlige myndigheter og organer som er etablert i nevnte medlemsstat, kan ilegges overtredelsesgebyrer.
9. Avhengig av medlemsstatenes rettsorden kan reglene for overtredelsesgebyrer anvendes på en slik måte at gebyrene ilegges av vedkommende nasjonale domstoler eller andre organer, alt etter hva som er relevant i disse medlemsstatene. Anvendelsen av disse reglene i disse medlemsstatene skal ha tilsvarende virkning.
10. Utøvelsen av myndighet i henhold til denne artikkelen bør være underlagt hensiktsmessige prosessuelle garantier i samsvar med unionsretten og nasjonal rett, herunder effektive rettsmidler og rettferdig rettergang.
11. Medlemsstatene skal hvert år rapportere til Kommisjonen om de overtredelsesgebyrene de har utstedt i løpet av det året, i samsvar med denne artikkelen, og om eventuelle tilknyttede tvister eller rettssaker.

Artikkel 100

Overtredelsesgebyrer til Unionens institusjoner, organer, kontorer og byråer

1. EUs datatilsyn kan ilegge overtredelsesgebyrer til de av Unionens institusjoner, organer, kontorer og byråer som faller inn under denne forordningens virkeområde. Når det treffes beslutning om hvorvidt det skal ilegges et overtredelsesgebyr, og om overtredelsesgebyrets størrelse i hvert enkelt tilfelle, skal alle relevante omstendigheter i den spesifikke situasjonen tas i betraktning, og det skal tas behørig hensyn til følgende:

- a) Karakteren, alvorlighetsgraden og varigheten av overtredelsen og av dens konsekvenser, tatt i betraktning det aktuelle KI-systemets formål og, dersom det er relevant, antallet berørte personer og omfanget av den skaden de har lidd.
 - b) Graden av ansvar hos EU-institusjonen, -organet, -kontoret eller -byrået, tatt i betraktning de tekniske og organisatoriske tiltakene de har iverksatt.
 - c) Eventuelle tiltak som EU-institusjonen, -organet, -kontoret eller -byrået har truffet for å begrense den skaden de berørte personene har lidd.
 - d) Graden av samarbeid med EUs datatilsyn for å bøte på overtredelsen og begrense de mulige negative virkningene av den, herunder etterlevelse av ethvert av de tiltakene som EUs datatilsyn tidligere har iverksatt overfor den aktuelle EU-institusjonen eller det aktuelle EU-organet, -kontoret eller -byrået i forbindelse med tilsvarende forhold.
 - e) Eventuelle lignende tidligere overtredelser begått av EU-institusjonen, -organet, -kontoret eller -byrået.
 - f) På hvilken måte EUs datatilsyn har fått kjennskap til overtredelsen, særlig om og i så fall i hvilken grad EU-institusjonen, -organet, -kontoret eller -byrået har underrettet om den.
 - g) EU-institusjonens, -organets, -kontorets eller -byråets årlige budsjett.
2. Ved manglende overholdelse av forbudet mot de formene for KI-praksis som er omhandlet i artikkel 5, skal det ilegges overtredelsesgebyrer på opptil 1 500 000 euro.
3. Ved KI-systemets manglende overholdelse av krav eller forpliktelser utenom om dem som er fastsatt i artikkel 5, skal det ilegges overtredelsesgebyrer på opptil 750 000 euro.
4. Før EUs datatilsyn treffer beslutninger i henhold til denne artikkelen, skal det gi EU-institusjonen, -organet, -kontoret eller -byrået som er gjenstand for den prosedyren det gjennomfører, mulighet til å uttale seg om den mulige overtredelsen. EUs datatilsyn skal bygge sine beslutninger utelukkende på elementer og forhold som de berørte partene har hatt mulighet til å uttale seg om. Eventuelle klager skal være nært knyttet til prosedyren.
5. De berørte partenes rett til å forsvare seg skal sikres fullt ut under prosedyren. De skal ha rett til innsyn i saksdokumentene til EUs datatilsyn, med forbehold for personers eller foretaks berettigede interesse av å bevare sine personopplysninger eller forretningshemmeligheter.
6. De midlene som samles inn ved ilegging av overtredelsesgebyrer i henhold til denne artikkelen, skal bidra til Unionens alminnelige budsjett. Overtredelsesgebyrene skal ikke hindre effektiv drift av EU-institusjonen, -organet, -kontoret eller -byrået som de ilegges.
7. EUs datatilsyn skal hvert år underrette Kommisjonen om de overtredelsesgebyrene det har ilagt i henhold til denne artikkelen, og om eventuelle tvister eller rettssaker det har innledet.

Artikkel 101

Overtredelsesgebyrer til leverandører av KI-modeller for allmenne formål

1. Kommisjonen kan ilegge leverandører av KI-modeller for allmenne formål overtredelsesgebyrer på opptil 3 % av deres samlede globale årsmøntsetning i det foregående regnskapsåret eller 15 000 000 euro, avhengig av hvilket beløp som er høyest, dersom Kommisjonen finner at leverandøren forsettlig eller uaktsomt har
- a) overtrådt de relevante bestemmelsene i denne forordningen,
 - b) unnlatt å etterkomme en anmodning om et dokument eller om informasjon i henhold til artikkel 91, eller gitt uriktig, ufullstendig eller villedende informasjon,
 - c) unnlatt å etterkomme en anmodning om et tiltak i henhold til artikkel 93,

- d) unnlatt å gi Kommisjonen tilgang til KI-modellen for allmenne formål med systemrisiko med henblikk på gjennomføring av en evaluering i henhold til artikkel 92.

Når overtredelsesgebyrets eller tvangsmulktens størrelse fastsettes, skal overtredelsens karakter, alvorlighet og varighet tas i betraktning, og det skal tas behørig hensyn til prinsippene om forholdsmessighet og rimelighet. Kommisjonen skal også ta hensyn til tilsagn som er gitt i samsvar med artikkel 93 nr. 3 eller i relevante regler for god praksis i samsvar med artikkel 56.

2. Før Kommisjonen vedtar beslutningen i henhold til nr. 1, skal den meddele sine foreløpige konklusjoner til leverandøren av KI-modellen for allmenne formål og gi den mulighet til å bli hørt.
3. Overtredelsesgebyrer som ilegges i samsvar med denne artikkelen, skal være virkningsfulle, stå i forhold til overtredelsen og virke avskrekkende.
4. Informasjon om overtredelsesgebyrer som ilegges i samsvar med denne artikkelen, skal også meddeles KI-rådet når det er relevant.
5. Den europeiske unions domstol skal ha ubegrenset domsmyndighet til å overprøve Kommisjonens beslutninger om fastsettelse av et overtredelsesgebyr etter denne artikkelen. Den kan oppheve, redusere eller øke overtredelsesgebyret som er ilagt.
6. Kommisjonen skal vedta gjennomføringsrettsakter som inneholder nærmere ordninger og prosessuelle garantier med henblikk på eventuell vedtakelse av beslutninger i henhold til nr. 1 i denne artikkelen. Disse gjennomføringsrettsaktene skal vedtas i samsvar med undersøkelsesprosedyren nevnt i artikkel 98 nr. 2.

KAPITTEL XIII

SLUTTBESTEMMELSER

Artikkel 102

Endring av forordning (EF) nr. 300/2008

I artikkel 4 nr. 3 i forordning (EF) nr. 300/2008 skal nytt ledd lyde:

«Ved vedtakelse av detaljerte tiltak knyttet til tekniske spesifikasjoner og prosedyrer for godkjenning og bruk av sikkerhetsutstyr i forbindelse med systemer for kunstig intelligens som definert i europaparlaments- og rådsforordning (EU) 2024/1689(*), skal det tas hensyn til kravene i kapittel III avsnitt 2 i nevnte forordning.

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler for 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 (forordningen 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 (EF) nr. 167/2013 skal nytt ledd lyde:

«Ved vedtakelse av delegerte rettsakter i samsvar med første ledd om systemer for kunstig intelligens som er sikkerhetskomponenter som definert i europaparlaments- og rådsforordning (EU) 2024/1689(*), skal det tas hensyn til kravene i kapittel III avsnitt 2 i nevnte forordning.

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler for 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 (forordningen 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 (EF) nr. 168/2013 skal nytt ledd lyde:

«Ved vedtakelse av delegerte rettsakter i samsvar med første ledd om systemer for kunstig intelligens som er sikkerhetskomponenter som definert i europaparlaments- og rådsforordning (EU) 2024/1689(*), skal det tas hensyn til kravene i kapittel III avsnitt 2 i nevnte forordning.

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler for 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 (forordningen 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 nytt nummer lyde:

«5. For systemer for kunstig intelligens som er sikkerhetskomponenter som definert i europaparlaments- og rådsforordning (EU) 2024/1689(*), skal Kommisjonen, når den utfører sin virksomhet i samsvar med nr. 1, og når den vedtar tekniske spesifikasjoner og prøvingsstandarter i samsvar med nr. 2 og 3, ta hensyn til kravene i kapittel III avsnitt 2 i nevnte forordning.

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler for 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 (forordningen 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 forordning (EU) 2016/797 skal nytt nummer lyde:

«12. «Ved vedtakelse av delegerte rettsakter i samsvar med nr. 1 og gjennomføringsrettsakter i samsvar med nr. 11 om systemer for kunstig intelligens som er sikkerhetskomponenter som definert i europaparlaments- og rådsforordning (EU) 2024/1689(*), skal det tas hensyn til kravene i kapittel III avsnitt 2 i nevnte forordning.

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler for 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 (forordningen 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 nytt nummer lyde:

«4. «Ved vedtakelse av delegerte rettsakter i samsvar med nr. 3 om systemer for kunstig intelligens som er sikkerhetskomponenter som definert i europaparlaments- og rådsforordning (EU) 2024/1689(*), skal det tas hensyn til kravene i kapittel III avsnitt 2 i nevnte forordning.

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler for 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 (forordningen om kunstig intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).».

Artikkel 108

Endring av forordning (EU) 2018/1139

I forordning (EU) 2018/1139 gjøres følgende endringer:

1) I artikkel 17 skal nytt nummer lyde:

«3. «Uten at det berører nr. 2, skal det ved vedtakelse av delegerte rettsakter i samsvar med nr. 1 om systemer for kunstig intelligens som er sikkerhetskomponenter som definert i europaparlaments- og rådsforordning (EU) 2024/1689(*), tas hensyn til kravene i kapittel III avsnitt 2 i nevnte forordning.

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler for 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 (forordningen om kunstig intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).».

2) I artikkel 19 skal nytt nummer lyde:

«4. «Ved vedtakelse av delegerte rettsakter i samsvar med nr. 1 og 2 om systemer for kunstig intelligens som er sikkerhetskomponenter som definert i europaparlaments- og rådsforordning (EU) 2024/1689, skal det tas hensyn til kravene i kapittel III avsnitt 2 i nevnte forordning.».

3) I artikkel 43 skal nytt nummer lyde:

«4. «Ved vedtakelse av delegerte rettsakter i samsvar med nr. 1 om systemer for kunstig intelligens som er sikkerhetskomponenter som definert i europaparlaments- og rådsforordning (EU) 2024/1689, skal det tas hensyn til kravene i kapittel III avsnitt 2 i nevnte forordning.».

4) I artikkel 47 skal nytt nummer lyde:

«3. «Ved vedtakelse av delegerte rettsakter i samsvar med nr. 1 og 2 om systemer for kunstig intelligens som er sikkerhetskomponenter som definert i europaparlaments- og rådsforordning (EU) 2024/1689, skal det tas hensyn til kravene i kapittel III avsnitt 2 i nevnte forordning.».

5) I artikkel 57 skal nytt ledd lyde:

«Ved vedtakelse av disse gjennomføringsrettsaktene om systemer for kunstig intelligens som er sikkerhetskomponenter som definert i europaparlaments- og rådsforordning (EU) 2024/1689, skal det tas hensyn til kravene i kapittel III avsnitt 2 i nevnte forordning.».

6) I artikkel 58 skal nytt nummer lyde:

«3. «Ved vedtakelse av delegerte rettsakter i samsvar med nr. 1 og 2 om systemer for kunstig intelligens som er sikkerhetskomponenter som definert i europaparlaments- og rådsforordning (EU) 2024/1689, skal det tas hensyn til kravene 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 nytt nummer lyde:

«3. «Ved vedtakelse av gjennomføringsrettsakter i samsvar med nr. 2 om systemer for kunstig intelligens som er sikkerhetskomponenter som definert i europaparlaments- og rådsforordning (EU) 2024/1689(*), skal det tas hensyn til kravene i kapittel III avsnitt 2 i nevnte forordning.

(*) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler for 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 (forordningen 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 vedlegget til europaparlaments- og rådsforordning (EU) 2020/1828⁽⁵⁸⁾ skal nytt nummer lyde:

«(68) Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelse av harmoniserte regler for 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 (forordningen om kunstig intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).».

Artikkel 111

KI-systemer som allerede er brakt i omsetning eller tatt i bruk, og KI-modeller for allmenne formål som allerede er brakt i omsetning

1. Uten at det berører anvendelsen av artikkel 5 som nevnt i artikkel 113 nr. 3 bokstav a), skal KI-systemer som er komponenter i de store IT-systemene som er opprettet 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 forordningen innen 31. desember 2030.

Det skal tas hensyn til kravene fastsatt i denne forordningen ved evalueringen av hvert av de store IT-systemene som er opprettet ved rettsaktene oppført i vedlegg X, og som skal gjennomføres som fastsatt i disse rettsaktene, og dersom rettsaktene erstattes eller endres.

2. Uten at det berører anvendelsen av artikkel 5 som nevnt i artikkel 113 nr. 3 bokstav a), får denne forordningen anvendelse på operatører av KI-systemer med høy risiko, bortsett fra systemene nevnt i nr. 1 i denne artikkelen, som er brakt i omsetning eller tatt i bruk før 2. august 2026, bare dersom det fra og med nevnte dato gjøres betydelige endringer i utformingen av disse systemene. I alle tilfeller skal leverandører og idriftsettere av KI-systemer med høy risiko som skal brukes av offentlige myndigheter, treffe de nødvendige tiltakene for å overholde kravene og forpliktelsene i denne forordningen innen 2. august 2030.

3. Leverandører av KI-modeller for allmenne formål som er brakt i omsetning før 2. august 2025, skal treffe de nødvendige tiltakene for å overholde forpliktelsene fastsatt i denne forordningen innen 2. august 2027.

⁽⁵⁸⁾ Europaparlaments- og rådsdirektiv (EU) 2020/1828 av 25. november 2020 om adgang til å anlegge gruppesøksmål for å ivareta forbrukernes kollektive interesser og om oppheving av direktiv 2009/22/EF (EUT L 409 av 4.12.2020, s. 1).

*Artikkel 112***Evaluering og revisjon**

1. Kommisjonen skal vurdere behovet for å endre listen i vedlegg III og listen over forbudte former for KI-praksis i artikkel 5 én gang i året etter ikrafttreddelsen av denne forordningen og fram til utløpet av perioden for delegering av myndighet fastsatt i artikkel 97. Kommisjonen skal sende konklusjonene fra denne vurderingen til Europaparlamentet og Rådet.
2. Kommisjonen skal innen 2. august 2028 og deretter hvert femte år framlegge for Europaparlamentet og Rådet en rapport om følgende:
 - a) Behovet for endringer som utvider eksisterende områderubrikker i vedlegg III eller tilføyer nye.
 - b) Endringer i listen over KI-systemer som krever ekstra åpenhetstiltak i artikkel 50.
 - c) Endringer som gjør tilsyns- og forvaltningssystemet mer effektivt.
3. Kommisjonen skal senest 2. august 2029 og deretter hvert fjerde år framlegge en rapport om vurderingen og revisjonen av denne forordningen for Europaparlamentet og Rådet. Rapporten skal omfatte en vurdering av håndhevelsesstrukturen og det mulige behovet for et EU-byrå for å avhjelpe eventuelle påviste mangler. På grunnlag av konklusjonene skal rapporten eventuelt ledsages av et forslag til endring av denne forordningen. Rapportene skal offentliggjøres.
4. I rapportene nevnt i nr. 2 skal det legges særlig vekt på følgende:
 - a) Status for de nasjonale vedkommende myndighetenes økonomiske, tekniske og menneskelige ressurser til effektivt å utføre oppgavene de er gitt ved denne forordningen.
 - b) Status for sanksjoner, særlig overtredelsesgebyrer som nevnt i artikkel 99 nr. 1, som medlemsstatene ilegger ved overtredelser av denne forordningen.
 - c) Vedtatte harmoniserte standarder og felles spesifikasjoner utarbeidet for å støtte denne forordningen.
 - d) Antall foretak som kommer inn på markedet etter ikrafttreddelsen av denne forordningen, og hvor mange av dem som er små og mellomstore bedrifter.
5. Kommisjonen skal innen 2. august 2028 vurdere hvordan KI-kontoret fungerer, om KI-kontoret har fått tilstrekkelige fullmakter og tilstrekkelig kompetanse til å utføre sine oppgaver, og om det vil være relevant og nødvendig å oppgradere KI-kontoret og dets håndhevelseskompetanse med henblikk på korrekt gjennomføring og håndhevelse av denne forordningen. Kommisjonen skal framlegge en rapport om sin vurdering for Europaparlamentet og Rådet.
6. Innen 2. august 2028 og deretter hvert fjerde år skal Kommisjonen framlegge en rapport om framdriften i utarbeidingen av standardiseringspublikasjoner om energieffektiv utvikling av KI-modeller for allmenne formål, og vurdere behovet for ytterligere forholdsregler eller tiltak, herunder bindende forholdsregler eller tiltak. Rapporten skal sendes til Europaparlamentet og Rådet og offentliggjøres.
7. Innen 2. august 2028 og deretter hvert tredje år skal Kommisjonen evaluere innvirkningen og effektiviteten av frivillige atferdsregler for å fremme anvendelse av kravene i vedlegg III avsnitt 2 på andre KI-systemer enn KI-systemer med høy risiko, herunder når det gjelder miljømessig bærekraft.
8. Ved anvendelsen av nr. 1–7 skal KI-rådet, medlemsstatene og nasjonale vedkommende myndigheter uten ugrunnet opphold gi Kommisjonen de opplysningene den anmoder om.
9. Når Kommisjonen gjennomfører evalueringene og revisjonene omhandlet i nr. 1–7, skal den ta hensyn til holdningene og konklusjonene fra Europaparlamentet, Rådet og andre relevante organer eller kilder.

10. Kommisjonen skal ved behov framlegge egnede forslag til endring av denne forordningen, særlig tatt i betraktning den teknologiske utviklingen, virkningene av KI-systemer på helse, sikkerhet og grunnleggende rettigheter, og i lys av framskrittene i informasjonssamfunnet.

11. For å veilede evalueringene og revisjonene omhandlet i nr. 1–7 i denne artikkelen skal KI-kontoret forplikte seg til å utarbeide en objektiv og deltakende metode for vurdering av risikonivåer som er basert på kriteriene angitt i de relevante artiklene, og oppføring av nye systemer på

- a) listen i vedlegg III, herunder utvidelse av eksisterende områderubrikker i nevnte vedlegg eller tilføyning av nye,
- b) listen over forbudte former for KI-praksis i artikkel 5 og
- c) listen over KI-systemer som krever ekstra åpenhetstiltak i samsvar med artikkel 50.

12. Ved enhver endring av denne forordningen i henhold til nr. 10, eller av relevante delegerte rettsakter eller gjennomføringsrettsakter, som gjelder sektorspesifikt EU-harmoniseringsregelverk oppført i avsnitt B i vedlegg I, skal det tas hensyn til de reguleringsmessige særtrekkene ved hver sektor og de eksisterende ordningene og myndighetene for forvaltning, samsvarsvurdering og håndhevelse som er opprettet i den enkelte sektoren.

13. Innen 2. august 2031 skal Kommisjonen gjennomføre en evaluering av håndhevelsen av denne forordningen og skal framlegge en rapport om dette for Europaparlamentet, Rådet og Den europeiske økonomiske og sosiale komité, der det tas hensyn til de første årene med anvendelse av denne forordningen. På grunnlag av konklusjonene skal rapporten, dersom det er relevant, ledsages av et forslag til endring av denne forordningen med hensyn til håndhevelsesstrukturen og behovet for et EU-byrå for å avhjelpe eventuelle påviste mangler.

Artikkel 113

Ikrafttredelse og anvendelse

Denne forordningen trer i kraft den 20. dagen etter at den er kunngjort i *Den europeiske unions tidende*.

Den får anvendelse fra 2. august 2026.

Imidlertid gjelder følgende:

- a) Kapittel I og II får anvendelse fra 2. februar 2025.
- b) Kapittel III avsnitt 4, kapittel V, kapittel VII og kapittel XII samt artikkel 78 får anvendelse fra 2. august 2025, med unntak av artikkel 101.
- c) Artikkel 6 nr. 1 og de tilsvarende forpliktelsene i denne forordningen får anvendelse fra 2. august 2027.

Denne forordningen er bindende i alle deler og kommer direkte til anvendelse i alle medlemsstater.

Utferdiget i Brussel 13. juni 2024.

For Europaparlamentet

R. METSOLA

President

For Rådet

M. MICHEL

Formann

VEDLEGG I

Liste over EU-harmoniseringsregelverk

Avsnitt A. Liste over EU-harmoniseringsregelverk som er basert på den nye rettslige rammen

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 sikkerhetskrav til 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 for 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 til bruk i eksplosjonsfarlige omgivelser (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 på markedet av radioutstyr 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 måleinstrumenter (EUT L 189 av 29.3.2014, s. 164).
8. Europaparlaments- og rådsforordning (EU) nr. 2016/424 av 9. mars 2016 om taubaneanlegg og om oppheving av direktiv 2000/9/EF (EUT L 81, av 31.3.2016).
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 gassapparater 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 samt 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).

Avsnitt B. Liste over annet EU-harmoniseringsregelverk

13. Europaparlaments- og rådsforordning (EF) nr. 300/2008 av 11. mars 2008 om felles bestemmelser om sikkerhet i 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 av og markedstilsyn for to- eller trehjuls kjøretøyer og firehjuls motorsykler (EUT L 60 av 2.3.2013, s. 52).
15. Europaparlaments- og rådsforordning (EU) nr. 167/2013 av 5. februar 2013 om godkjenning av og markedstilsyn for jordbruks- 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 samtrafikkveien i Den europeiske unions jernbanesystem (EUT L 138 av 26.5.2016, s. 44).
18. Europaparlaments- og rådsforordning (EU) 2018/858 av 30. mai 2018 om godkjenning av og markedstilsyn med motorvogner og deres tilhengere samt systemer, komponenter og separate tekniske enheter til 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 deres tilhengere, og av systemer, komponenter og separate tekniske enheter beregnet på slike kjøretøyer, med hensyn til deres generelle sikkerhet og beskyttelse av personer i motorvognen og sårbare trafikanter, om endring av europaparlaments- og rådsforordning (EU) 2018/858 og om oppheving av europaparlaments- og rådsforordning (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. 1009/2010, (EU) nr. 19/2011, (EU) nr. 109/2011, (EU) nr. 458/2011, (EU) nr. 65/2012, (EU) nr. 130/2012, (EU) nr. 347/2012, (EU) nr. 351/2012, (EU) nr. 1230/2012 og (EU) 2015/166 (EUT L 325 av 16.12.2019, s. 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 flysikkerhetsbyrå, og om endring av europaparlaments- og rådsforordning (EF) nr. 2111/2005, (EF) nr. 1008/2008, (EU) nr. 996/2010 og (EU) nr. 376/2014, og europaparlaments- og rådsdirektiv 2014/30/EU og 2014/53/EU, samt 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), i den grad det gjelder konstruksjon, produksjon og omsetning av luftfartøyer som nevnt i artikkel 2 nr. 1 bokstav a) og b) i den forordningen, med hensyn til ubemannede luftfartøyer og deres motorer, propeller, deler og utstyr til fjernstyring.

VEDLEGG II

Liste over straffbare handlinger omhandlet i artikkel 5 nr. 1 første ledd bokstav h) iii)

Straffbare handlinger omhandlet i artikkel 5 nr. 1 første ledd bokstav h) iii):

- terrorhandlinger
 - menneskehandel
 - seksuell utnytting av barn samt barnepornografi
 - ulovlig handel med narkotika eller psykotrope stoffer
 - ulovlig handel med våpen, ammunisjon eller eksplosiver
 - drap, alvorlig kroppsskade
 - ulovlig handel med organer eller vev fra mennesker
 - ulovlig handel med kjernefysisk eller radioaktivt materiale
 - kidnapping, ulovlig frihetsberøvelse eller gisseltaking
 - forbrytelser som faller inn under Den internasjonale straffedomstols jurisdiksjon
 - kapring av luftfartøyer eller skip
 - voldtekt
 - miljøkriminalitet
 - organisert eller væpnet ran
 - sabotasje
 - deltakelse i en kriminell organisasjon som er involvert i en eller flere av de straffbare handlingene nevnt ovenfor
-

VEDLEGG III

KI-systemer med høy risiko omhandlet i artikkel 6 nr. 2

KI-systemer med høy risiko i henhold til artikkel 6 nr. 2 er de KI-systemene som er oppført under et av følgende områder:

1. Biometri, i den utstrekning bruken er tillatt i henhold til relevant unionsrett eller nasjonal rett:
 - a) Systemer for biometrisk fjernidentifikasjon.

Dette skal ikke omfatte KI-systemer som er ment å brukes til biometrisk verifisering, og hvis eneste formål er å bekrefte at en bestemt fysisk person er den som han eller hun utgir seg for å være.
 - b) KI-systemer som er beregnet på å brukes til biometrisk kategorisering ut fra sensitive eller beskyttede egenskaper eller kjennetegn basert på utledning av disse egenskapene eller kjennetegnene.
 - c) KI-systemer beregnet på å brukes til følelsesgjenkjenning.
2. Kritisk infrastruktur: KI-systemer som er beregnet på å brukes som sikkerhetskomponenter i forvaltning og drift av kritisk digital infrastruktur, i veitrafikk eller i forsyning av vann, gass, varme eller elektrisitet.
3. Utdanning og yrkesrettet opplæring:
 - a) KI-systemer beregnet på å brukes til å bestemme adgang eller opptak eller til å anviser fysiske personer til institusjoner for utdanning eller yrkesrettet opplæring på alle nivåer.
 - b) KI-systemer beregnet på å brukes til å evaluere læringsutbytte, også når læringsutbyttet brukes for å styre fysiske personers læringsprosess i institusjoner for utdanning og yrkesrettet opplæring på alle nivåer.
 - c) KI-systemer beregnet på å brukes til å vurdere det hensiktsmessige utdanningsnivået som en person vil motta eller gis tilgang til, i forbindelse med eller innenfor rammen av institusjoner for utdanning og yrkesrettet opplæring på alle nivåer.
 - d) KI-systemer beregnet på å brukes til å overvåke og påvise forbudt atferd hos studenter under prøver i forbindelse med eller innenfor rammen av institusjoner for utdanning og yrkesrettet opplæring på alle nivåer.
4. Sysselsetting, arbeidsledelse og tilgang til selvstendig næringsvirksomhet:
 - a) KI-systemer beregnet på å brukes til rekruttering eller utvelgelse av fysiske personer, særlig for å publisere målrettede stillingsannonser, analysere og filtrere jobbsøknader og evaluere kandidater.
 - b) KI-systemer beregnet på å brukes for å treffe beslutninger som påvirker vilkårene for arbeidsrelaterte forhold, forfremmelser eller oppsigelser i arbeidsrelaterte kontraktsforhold, til å fordele oppgaver på grunnlag av individuell atferd, personlighetstrekk eller egenskaper eller til å overvåke og evaluere prestasjonene og atferden til personer i slike forhold.
5. Tilgang til og utnyttelse av vesentlige private tjenester og vesentlige offentlige tjenester og ytelser:
 - a) KI-systemer beregnet på å brukes av offentlige myndigheter eller på vegne av offentlige myndigheter for å vurdere om fysiske personer har rett til vesentlige offentlige bistandsytelser og -tjenester, herunder helsetjenester, samt for å gi, redusere, tilbakekalle eller kreve tilbake slike ytelser og tjenester.
 - b) KI-systemer beregnet på å brukes til å evaluere fysiske personers kredittverdighet eller bestemme deres kredittskår, med unntak av KI-systemer som brukes til å avdekke økonomisk bedrageri.
 - c) KI-systemer beregnet på å brukes til risikovurdering og prissetting i forbindelse med livsforsikring og helseforsikring for fysiske personer.

- d) KI-systemer beregnet på å brukes, herunder av politiet, brannvesenet og helsevesenet, til å evaluere og klassifisere nød-anrop fra fysiske personer eller til å sende ut eller fastsette prioritet for utsending av beredskapstjenester, samt systemer for pasientsortering for førstehjelp.
6. Rettshåndhevelse, i den utstrekning bruken er tillatt i henhold til relevant unionsrett eller nasjonal rett:
- a) KI-systemer beregnet på 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) KI-systemer beregnet på å brukes av eller på vegne av rettshåndhevende myndigheter eller av Unionens institusjoner, organer, kontorer eller byråer til støtte for rettshåndhevende myndigheter som løgndetektorer eller lignende verktøy.
 - c) KI-systemer beregnet på å brukes av eller på vegne av rettshåndhevende myndigheter eller av Unionens institusjoner, organer, kontorer eller byråer til støtte for rettshåndhevende myndigheter for å vurdere påliteligheten av bevis i forbindelse med etterforskning eller rettsforfølgning av straffbare handlinger.
 - d) KI-systemer 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 for at en fysisk person begår eller på nytt begår en straffbar handling, ikke bare 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 egenskaper eller fysiske personers eller grupperes tidligere kriminelle atferd.
 - e) KI-systemer beregnet på å brukes av eller på vegne av 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. Migrasjons-, asyl- og grensekontrollforvaltning, i den utstrekning bruken er tillatt i henhold til relevant unionsrett eller nasjonal rett:
- a) KI-systemer beregnet på å brukes av eller på vegne av vedkommende nasjonale myndigheter eller av Unionens institusjoner, organer, kontorer eller byråer som løgndetektorer eller lignende verktøy.
 - b) KI-systemer 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 helseis risiko som utgjøres av en fysisk person som har til hensikt å reise inn på eller har reist inn på en medlemsstats territorium.
 - c) KI-systemer 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 klager i den forbindelse, med hensyn til om fysiske personer som søker, er berettiget til slik status, herunder tilhørende vurderinger av påliteligheten av bevis.
 - d) KI-systemer 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 for det formålet å oppdage, gjenkjenne eller identifisere fysiske personer, med unntak av verifisering av reisedokumenter.
8. Rettspleie og demokratiske prosesser:
- a) KI-systemer beregnet på å brukes av en rettsmyndighet eller på dennes vegne for å bistå en rettsmyndighet med å undersøke og tolke fakta og lovgivning og med å anvende lovgivningen på konkrete saksforhold, eller brukes på lignende måte i alternativ tvisteløsning.

- b) KI-systemer beregnet på å brukes til å påvirke utfallet av et valg eller en folkeavstemning eller fysiske personers stemmeatferd når de utøver sin stemmerett ved valg eller folkeavstemninger. Dette omfatter ikke KI-systemer hvis utdata 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.
-

UOFFISIELL OVERSETTELSE

VEDLEGG IV

Teknisk dokumentasjon nevnt i artikkel 11 nr. 1

Den tekniske dokumentasjonen nevnt i artikkel 11 nr. 1 skal inneholde minst følgende opplysninger, alt etter hva som er aktuelt for det relevante KI-systemet:

1. En generell beskrivelse av KI-systemet, herunder
 - a) dets tiltenkte formål, leverandørens navn og versjonen av systemet, som avspeiler sammenhengen med tidligere versjoner,
 - b) dersom det er relevant, hvordan KI-systemet samhandler med eller kan brukes til å samhandle med maskinvare eller programvare, herunder andre KI-systemer, som ikke er en del av selve KI-systemet,
 - c) versjonene av relevant programvare eller fastvare og eventuelle krav med hensyn til versjonsoppdateringer,
 - d) en beskrivelse av alle formene som KI-systemet bringes i omsetning eller tas i bruk i, for eksempel programvarepakker innebygd i maskinvare, nedlastinger eller API-er,
 - e) en beskrivelse av maskinvaren som KI-systemet er beregnet på å kjøres på,
 - f) dersom KI-systemet er en komponent i produkter, fotografier eller illustrasjoner som viser disse produktenes ytre kjenetegn, merking og interne utforming,
 - g) en grunnleggende beskrivelse av brukergrensesnittet som gjøres tilgjengelig for idriftsetteren,
 - h) en bruksanvisning for idriftsetteren og, dersom det er relevant, en grunnleggende beskrivelse av brukergrensesnittet som gjøres tilgjengelig for idriftsetteren.
2. En detaljert beskrivelse av elementene i KI-systemet og av prosessen for å utvikle det, herunder
 - a) metodene og trinnene i utviklingen av KI-systemet, herunder, dersom det er relevant, bruk av forhåndstrengte systemer eller verktøy levert av tredjeparter, og hvordan disse er blitt brukt, integrert eller endret av leverandøren,
 - b) systemets konstruksjonsspesifikasjoner, det vil si den generelle logikken i KI-systemet og algoritmene, de viktigste konstruksjonsvalgene, herunder begrunnelsen for dem samt de antakelsene som er gjort, også med hensyn til personer eller grupper av personer som systemet er ment å brukes på, de viktigste klassifiseringsvalgene, hva systemet er konstruert for å optimere, og relevansen av de forskjellige parametrene, en beskrivelse av systemets forventede utdata og utdatakvalitet samt beslutningene om eventuelle kompromisser med hensyn til de tekniske løsningene som er tatt i bruk for å oppfylle kravene i kapittel III avsnitt 2,
 - c) en beskrivelse av systemarkitekturen som forklarer hvordan programvarekomponenter bygger på eller inngår i hverandre og er integrert i den samlede databehandlingen, samt regnekraften som er brukt til å utvikle, trene, teste og validere KI-systemet,
 - d) dersom det er relevant, datakravene i form av datablader som beskriver treningsmetodene, treningsteknikkene og treningsdatasettene som er brukt, herunder en generell beskrivelse av disse datasettene og informasjon om deres opprinnelse, omfang og viktigste egenskaper, hvordan dataene er innhentet og valgt ut, merkingsprosedyrer (for eksempel for overvåket læring) og datarensingsmetoder (for eksempel påvisning av ekstremverdier),
 - e) vurdering av de tiltakene for menneskelig tilsyn som er nødvendige i samsvar med artikkel 14, herunder en vurdering av de tekniske tiltakene som er nødvendige for å lette idriftsetternes tolkning av utdataene fra KI-systemene, i samsvar med artikkel 13 nr. 3 bokstav d),
 - f) dersom 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, målene som er brukt for nøyaktighet, robusthet og samsvar med andre relevante krav i kapittel III avsnitt 2, samt potensielt diskriminerende virkninger, testlogger og alle testrapporter, datert og underskrevet av de ansvarlige personene, herunder med hensyn til forhåndsbestemte endringer som nevnt i bokstav f),

- h) cybersikkerhetstiltak som er truffet.
3. Detaljert informasjon om overvåking, drift og kontroll av KI-systemet, særlig med hensyn til dets kapabiliteter og ytelsesbegrensninger, herunder nøyaktighetsgraden for bestemte personer eller grupper av personer som systemet er ment å brukes på, og det samlede forventede nøyaktighetenivået i forhold til det tiltenkte formålet, forutsigbare utilsiktede resultater og kilder til risiko for helse, sikkerhet og grunnleggende rettigheter og for at det skjer diskriminering, på bakgrunn av KI-systemets tiltenkte formål, de tiltakene for menneskelig tilsyn som er nødvendige i samsvar med artikkel 14, herunder de tekniske tiltakene som er iverksatt for å lette idriftsetternes tolkning av utdataene fra KI-systemene, samt spesifikasjoner for inndata, alt etter hva som er relevant.
 4. En beskrivelse av egnetheten av ytelsesmålene for det spesifikke KI-systemet.
 5. En detaljert beskrivelse av risikohåndteringssystemet i samsvar med artikkel 9.
 6. En beskrivelse av relevante endringer som leverandøren har gjort i systemet i løpet av dets livssyklus.
 7. En liste over de harmoniserte standardene som er anvendt helt eller delvis, og som det er offentliggjort henvisninger til i *Den europeiske unions tidende*. Dersom det ikke er anvendt noen slike harmoniserte standarder, en detaljert beskrivelse av de løsningene som er valgt for å oppfylle de grunnleggende 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 omhandlet i artikkel 47.
 9. En detaljert beskrivelse av systemet som i samsvar med artikkel 72 er innført for å evaluere KI-systemets ytelse i fasen etter at det er brakt i omsetning, herunder planen for overvåking etter omsetning nevnt i artikkel 72 nr. 3.
-

VEDLEGG V

EU-samsvarserklæring

EU-samsvarserklæringen omhandlet i artikkel 47 skal inneholde all følgende informasjon:

1. KI-systemets navn og type og enhver annen entydig referanse som gjør det mulig å identifisere og spore KI-systemet.
2. Navn og adresse til leverandøren eller, dersom det er relevant, leverandørens bemyndigede representant.
3. En erklæring om at EU-samsvarserklæringen omhandlet i artikkel 47 er utstedt på leverandørens eneansvar.
4. En erklæring om at KI-systemet er i samsvar med denne forordningen og eventuelt med annet relevant unionsrett som inneholder bestemmelser om utstedelse av EU-samsvarserklæringen omhandlet i artikkel 47.
5. Når et KI-system innbefatter behandling av personopplysninger, en erklæring om at KI-systemet er i samsvar med forordning (EU) 2016/679 og (EU) 2018/1725 samt direktiv (EU) 2016/680.
6. Henvisninger til relevante harmoniserte standarder som er brukt, eller andre felles spesifikasjoner som det erklæres samsvar med.
7. Dersom det er relevant, det meldte organets navn og identifikasjonsnummer, en beskrivelse av samsvarsvurderingsprosedyren som er gjennomført, og identifikasjon av sertifikatet som er utstedt.
8. Sted og dato for utstedelse av erklæringen, underskriverens navn og stilling, opplysning om hvem vedkommende har underskrevet på vegne av, samt underskrift.

—

*VEDLEGG VI***Samsvarsvurderingsprosedyre basert på internkontroll**

1. Samsvarsvurderingsprosedyren basert på internkontroll er samsvarsvurderingsprosedyren beskrevet i nr. 2, 3 og 4.
 2. Leverandøren verifiserer at det innførte kvalitetsstyringssystemet oppfyller kravene i artikkel 17.
 3. Leverandøren undersøker informasjonen i den tekniske dokumentasjonen for å vurdere om KI-systemet oppfyller de relevante grunnleggende kravene i kapittel III avsnitt 2.
 4. Leverandøren verifiserer også at utformings- og utviklingsprosessen for KI-systemet og overvåkingen av KI-systemet etter omsetning i samsvar med artikkel 72 er i tråd med den tekniske dokumentasjonen.
-

UOFFISIELL OVERSETTELSE

VEDLEGG VII

Samsvar basert på en vurdering av kvalitetsstyringssystemet og av den tekniske dokumentasjonen

1. Innledning

Samsvar basert på en vurdering av kvalitetsstyringssystemet og av den tekniske dokumentasjonen er samsvarsvurderingsprosedyren beskrevet i nr. 2–5.

2. Oversikt

Det godkjente kvalitetsstyringssystemet for utformingen, utviklingen og testingen av KI-systemer i henhold til artikkel 17 skal undersøkes i samsvar med nr. 3 og være gjenstand for tilsyn som angitt i nr. 5. Den tekniske dokumentasjonen om KI-systemet skal undersøkes i samsvar med nr. 4.

3. Kvalitetsstyringssystem

3.1. Leverandørens søknad skal inneholde

- a) leverandørens navn og adresse og, dersom søknaden inngis av en bemyndiget representant, også dennes navn og adresse,
- b) en liste over de KI-systemene som omfattes av det samme kvalitetsstyringssystemet,
- c) den tekniske dokumentasjonen om hvert KI-system som omfattes av det samme kvalitetsstyringssystemet,
- d) dokumentasjonen om kvalitetsstyringssystemet, som skal omfatte alle aspektene nevnt i artikkel 17,
- e) en beskrivelse av prosedyrene som er innført for å sikre at kvalitetsstyringssystemet forblir hensiktsmessig og effektivt,
- f) en skriftlig erklæring om at samme søknad ikke er levert til et annet meldt organ.

3.2. Kvalitetsstyringssystemet skal vurderes av det meldte organet, som skal avgjøre om det oppfyller kravene nevnt i artikkel 17.

Leverandøren eller leverandørens bemyndigede representant skal underrettes om avgjørelsen.

Underretningen skal inneholde konklusjonene fra vurderingen av kvalitetsstyringssystemet og en begrunnelse for avgjørelsen.

3.3. Når kvalitetsstyringssystemet er godkjent, skal leverandøren fortsette å gjennomføre det og vedlikeholde det, slik at det forblir hensiktsmessig og effektivt.

3.4. Leverandøren skal underrette det meldte organet om enhver planlagt endring av det godkjente kvalitetsstyringssystemet eller i listen over KI-systemer som omfattes av det.

De foreslåtte endringene skal undersøkes av det meldte organet, som skal vurdere foreslåtte endringer og avgjøre om det endrede kvalitetsstyringssystemet fortsatt oppfyller kravene nevnt i nr. 3.2, eller om det kreves en ny vurdering.

Det meldte organet skal underrette leverandøren om sin avgjørelse. Underretningen skal inneholde konklusjonene fra undersøkelsen og en begrunnelse for avgjørelsen.

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 å få vurdert den tekniske dokumentasjonen om det KI-systemet som leverandøren har til hensikt å bringe i omsetning eller ta i bruk, og som omfattes av kvalitetsstyringssystemet omhandlet i nr. 3.

4.2. Søknaden skal inneholde

- a) leverandørens navn og adresse,
- b) en skriftlig erklæring om at samme søknad ikke er inngitt til et annet meldt organ,
- c) den tekniske dokumentasjonen omhandlet i vedlegg IV.

- 4.3. Den tekniske dokumentasjonen skal undersøkes av det meldte organet. Dersom 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 trenings-, validerings- og testdatasettene som er brukt, herunder, dersom det er relevant og omfattet av sikkerhetstiltak, gjennom API-er eller andre relevante tekniske midler og verktøy som muliggjør fjerntilgang.
- 4.4. Når det meldte organet undersøker den tekniske dokumentasjonen, kan det kreve at leverandøren framlegger ytterligere dokumentasjon eller gjennomfører ytterligere tester for at det skal kunne gjøres en tilfredsstillende vurdering av om KI-systemet oppfyller kravene i kapittel III avsnitt 2. Dersom det meldte organet ikke er tilfreds med de testene som leverandøren har utført, skal det selv utføre egnede tester direkte, alt etter hva som er relevant.
- 4.5. Dersom det er nødvendig for å vurdere om KI-systemet med høy risiko oppfyller kravene i kapittel III avsnitt 2, etter at alle andre rimelige metoder for å kontrollere samsvar er forsøkt og har vist seg å være utilstrekkelige, og etter en begrunnet anmodning, skal det meldte organet også få tilgang til KI-systemets treningsmodeller og trente modeller, herunder dets relevante parametere. Slik tilgang skal omfattes av gjeldende unionsrett om vern av immaterielle rettigheter og forretningshemmeligheter.
- 4.6. Leverandøren eller leverandørens bemyndigede representant skal underrettes om det meldte organets avgjørelse. Underretningen skal inneholde konklusjonene fra undersøkelsen av den tekniske dokumentasjonen og en begrunnelse for avgjørelsen.

Dersom KI-systemet er i samsvar med kravene i kapittel III avsnitt 2, skal det meldte organet utstede et EU-sertifikat for vurdering av teknisk dokumentasjon. Sertifikatet skal inneholde produsentens navn og adresse, konklusjonene fra undersøkelsen, eventuelle vilkår for dets gyldighet og de dataene som er nødvendige for å identifisere KI-systemet.

Sertifikatet og dets vedlegg skal inneholde alle opplysninger som er nødvendige for å vurdere om KI-systemet er i samsvar med kravene, og for å kontrollere KI-systemet under bruk dersom det er relevant.

Dersom KI-systemet ikke er i samsvar med kravene i kapittel III avsnitt 2, skal det meldte organet avslå å utstede et EU-sertifikat for vurdering av teknisk dokumentasjon, underrette søkeren om dette og gi en detaljert begrunnelse for avslaget.

Dersom KI-systemet ikke oppfyller kravene som gjelder dataene som er brukt til å trene det, må KI-systemet trenes på nytt før det søkes om en ny samsvarsvurdering. I så fall skal det meldte organets begrunnede avgjørelse om ikke å utstede EU-sertifikatet for vurdering av teknisk dokumentasjon inneholde særskilte betraktninger om kvaliteten på dataene som er brukt til å trene KI-systemet, særlig om grunnene til at de ikke samsvarer med kravene.

- 4.7. Enhver endring i KI-systemet som kan påvirke KI-systemets samsvar med kravene eller dets tiltenkte formål, skal vurderes av det meldte organet som har utstedt EU-sertifikatet for vurdering av teknisk dokumentasjon. Dersom leverandøren har til hensikt å foreta noen av de ovennevnte endringene eller på annen måte blir oppmerksom på at slike endringer er foretatt, skal den underrette det meldte organet om dette. De planlagte endringene skal vurderes av det meldte organet, som skal avgjøre om endringene krever at det utføres en ny samsvarsvurdering i samsvar med artikkel 43 nr. 4, eller om de kan angis i et tillegg til EU-sertifikatet for vurdering av teknisk dokumentasjon. I sistnevnte tilfelle skal det meldte organet vurdere endringene, underrette leverandøren om sin avgjørelse og, dersom endringene godkjennes, utstede et tillegg til leverandørens EU-sertifikat for vurdering av teknisk dokumentasjon.
5. Tilsyn med det godkjente kvalitetsstyringssystemet
 - 5.1. Formålet med det meldte organets tilsyn som omhandlet i nr. 3 er å sikre at leverandøren behørig overholder vilkårene i det godkjente kvalitetsstyringssystemet.
 - 5.2. Med henblikk på vurdering skal leverandøren gi det meldte organet adgang til lokalene der konstruksjonen, utviklingen og testingen av KI-systemene finner sted. Leverandøren skal videre dele alle nødvendige opplysninger med det meldte organet.
 - 5.3. Det meldte organet skal gjennomføre periodiske revisjoner for å sikre at leverandøren vedlikeholder og bruker kvalitetsstyringssystemet, og skal framlegge en revisjonsrapport for leverandøren. I forbindelse med disse revisjonene kan det meldte organet gjennomføre ytterligere tester av de KI-systemene der det er utstedt et EU-sertifikat for vurdering av teknisk dokumentasjon.

VEDLEGG VIII

Opplysninger som skal gis ved registrering av KI-systemer med høy risiko i samsvar med artikkel 49

Avsnitt A – Opplysninger som skal gis av leverandører av KI-systemer med høy risiko i samsvar med artikkel 49 nr. 1

Følgende opplysninger skal gis og deretter holdes oppdatert med hensyn til KI-systemer med høy risiko som skal registreres i samsvar med artikkel 49 nr. 1:

1. Navn, adresse og kontaktopplysninger til leverandøren.
2. Dersom opplysningene gis av en annen person på vegne av leverandøren: navn, adresse og kontaktopplysninger til den personen.
3. Navn, adresse og kontaktopplysninger til den bemyndigede representanten, dersom det er relevant.
4. KI-systemets handelsnavn og enhver annen entydig referanse som gjør det mulig å identifisere og spore KI-systemet.
5. En beskrivelse av det tiltenkte formålet med KI-systemet og med komponentene og funksjonene som støttes gjennom dette KI-systemet.
6. En grunnleggende og kortfattet beskrivelse av informasjonen som brukes av systemet (data, inndata), og av systemets driftslogikk.
7. KI-systemets status (på markedet, i bruk, bringes ikke lenger i omsetning/ ikke lenger i bruk, tilbakekalt).
8. Type, nummer og utløpsdato for sertifikatet som er utstedt av det meldte organet, samt det meldte organets navn eller identifikasjonsnummer dersom det er relevant.
9. En skannet kopi av sertifikatet nevnt i nr. 8 dersom det er relevant.
10. Eventuelle medlemsstater der KI-systemet er brakt i omsetning, tatt i bruk eller gjort tilgjengelig i Unionen.
11. En kopi av EU-samsvarserklæringen omhandlet i artikkel 47.
12. En elektronisk bruksanvisning. Denne informasjonen skal ikke gis for KI-systemer med høy risiko på områdene rettshåndhevelse eller migrasjons-, asyl- og grensekontrollforvaltning som omhandlet i vedlegg III nr. 1, 6 og 7.
13. En nettside der det finnes ytterligere informasjon (valgfritt).

Avsnitt B – Opplysninger som skal gis av leverandører av KI-systemer med høy risiko i samsvar med artikkel 49 nr. 2

Følgende opplysninger skal gis og deretter holdes oppdatert med hensyn til KI-systemer som registreres i samsvar med artikkel 49 nr. 2:

1. Navn, adresse og kontaktopplysninger til leverandøren.
2. Dersom opplysningene gis av en annen person på vegne av leverandøren: navn, adresse og kontaktopplysninger til den personen.
3. Navn, adresse og kontaktopplysninger til den bemyndigede representanten, dersom det er relevant.
4. KI-systemets handelsnavn og enhver annen entydig referanse som gjør det mulig å identifisere og spore KI-systemet.
5. En beskrivelse av KI-systemets tiltenkte formål.
6. Det eller de vilkårene i artikkel 6 nr. 3 som gjør at KI-systemet ikke anses som et system med høy risiko.
7. Et kort sammendrag av grunnene til at KI-systemet ikke anses som et system med høy risiko ved anvendelse av prosedyren i artikkel 6 nr. 3.
8. KI-systemets status (på markedet, i bruk, bringes ikke lenger i omsetning/ ikke lenger i bruk, tilbakekalt).
9. Eventuelle medlemsstater der KI-systemet er brakt i omsetning, tatt i bruk eller gjort tilgjengelig i Unionen.

Avsnitt C – Opplysninger som skal gis av leverandører av KI-systemer med høy risiko i samsvar med artikkel 49 nr. 3

Følgende opplysninger skal gis og deretter holdes oppdatert med hensyn til KI-systemer med høy risiko som skal registreres i samsvar med artikkel 49 nr. 3:

1. Navn, adresse og kontaktopplysninger til idriftsetteren.
2. Navn, adresse og kontaktopplysninger til personen som gir opplysningene på vegne av idriftsetteren.
3. Nettdressen til leverandørens registrering av KI-systemet i EU-databasen.
4. Et sammendrag av funnene fra konsekvensanalysen om grunnleggende rettigheter gjennomført i samsvar med artikkel 27.
5. Et sammendrag av vurderingen av personvernkonsekvenser gjennomført 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 forordningen, dersom det er relevant.

UOFFISIELL OVERSETTELSE

VEDLEGG IX

Opplysninger som skal gis ved registrering av KI-systemer med høy risiko oppført i vedlegg III med hensyn til testing under virkelige forhold i samsvar med artikkel 60

Følgende opplysninger skal gis og deretter holdes oppdatert med hensyn til testing under virkelige forhold som skal registreres i samsvar med artikkel 60:

1. Et unikt EU-identifikasjonsnummer for testingen under virkelige forhold.
 2. Navn og kontaktopplysninger til leverandøren eller den prospektive leverandøren og til idriftsetterne som deltar i testingen under virkelige forhold.
 3. En kort beskrivelse av KI-systemet, dets tiltenkte formål og annen informasjon som er nødvendig for å kunne identifisere systemet.
 4. Et sammendrag av de viktigste særtrekkene ved planen for testing under virkelige forhold.
 5. Informasjon om suspensjon eller avslutning av testingen under virkelige forhold.
-

VEDLEGG X

EU-rettsakter om store IT-systemer på området for frihet, sikkerhet og rettferdighet

1. Schengen-informasjonssystemet

- 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) på området inn- og utreisekontroll, om endring av konvensjonen om gjennomføring av Schengen-avtalen og om endring av 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) innenfor politisamarbeid og strafferettslig samarbeid, om endring og oppheving av rådsbeslutning 2007/533/JI S og om oppheving av europaparlaments- og rådsforordning (EF) nr. 1986/2006 og rådsbeslutning 2010/261/EU (EUT L 312 av 7.12.2018, s. 56).

2. Visuminformasjonssystemet

- 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 om endring av europaparlaments- og rådsforordning (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 og om oppheving av rådsvedtak 2004/512/EF og rådsbeslutning 2008/633/JIS med henblikk på reform av visuminformasjonssystemet (EUT L 248 av 13.7.2021, s. 11).

3. Eurodac

Europaparlaments- og rådsforordning (EU) 2024/1358 av 14. mai 2024 om opprettelse av «Eurodac» for sammenligning av biometriske opplysninger for effektiv anvendelse av europaparlaments- og rådsforordning (EU) 2024/1351 og (EU) 2024/1350 og rådsdirektiv 2001/55/EF og for å identifisere en tredjelandsborger eller statsløs med ulovlig opphold, og om anmodninger om sammenligning med Eurodac-opplysninger fra medlemsstatenes rettshåndhevende myndigheter og Euro-pol 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, 22.5.2024, ELI: <http://data.europa.eu/eli/reg/2024/1358/oj>).

4. Inn- og utreisestystem

Europaparlaments- og rådsforordning (EU) 2017/2226 av 30. november 2017 om etablering av et inn- og utreisestystem (EES) for å registrere inn- og utreisedata og data om avvisning av innreise for tredjelandsborgere som krysser medlemsstatenes ytre grenser og for å fastslå vilkårene for tilgang til EES for rettshåndhevende formål, 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. Det europeiske systemet for reiseinformasjon og framreisetillatelse

- a) Europaparlaments- og rådsforordning (EU) nr. 2018/1240 av 12. september 2018 om etablering av et europeisk system for reiseinformasjon og framreisetillatelse (ETIAS) og om endring av forordning (EF) 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 henblikk på etablering av et europeisk system for innreiseinformasjon og framreisetillatelse (ETIAS) (EUT L 236 av 19.9.2018, s. 72).

6. Det europeiske systemet for opplysninger fra strafferegistre om tredjelandsborgere og statsløse personer

Europaparlaments- og rådsforordning (EU) 2019/816 av 17. april 2019 om opprettelse av et sentralisert system for å identifisere medlemsstater som innehar informasjon om domfellelser mot tredjelandsborgere og statsløse personer (ECRIS-TCN), for å utfylle det europeiske systemet for opplysninger om strafferegistre, 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-informasjonssystemene på området grenser og visum og om endring av europaparlaments- og rådsforordning (EF) nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 og (EU) 2018/1861 og rådsvedtak 2004/512/EF og rådsbeslutning 2008/633/JIS (EUT L 135 av 22.5.2019, s. 27).
- b) Europaparlaments- og rådsforordning (EU) 2019/818 av 20. mai 2019 om fastsettelse av en ramme for interoperabilitet mellom EUs informasjonssystemer på området politisamarbeid og samarbeid mellom rettshåndhevende myndigheter, 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).

—

UOFFISIELL OVERSETTELSE

VEDLEGG XI

Teknisk dokumentasjon nevnt i artikkel 53 nr. 1 bokstav a) – teknisk dokumentasjon for leverandører av KI-modeller for allmenne formål

Avsnitt 1

Opplysninger som skal gis av alle leverandører av KI-modeller for allmenne formål

Den tekniske dokumentasjonen nevnt i artikkel 53 nr. 1 skal inneholde minst følgende opplysninger, i samsvar med modellens størrelse og risikoprofil:

1. En generell beskrivelse av KI-modellen for allmenne formål, herunder
 - a) oppgavene som modellen er ment å utføre, og hvilken type og art av KI-systemer den kan integreres i,
 - b) de gjeldende retningslinjene for akseptabel bruk,
 - c) utgivelsesdatoen og distribusjonsmetodene,
 - d) arkitekturen og antallet parametere,
 - e) modaliteten (for eksempel tekst eller bilde) og formatet for inndata og utdata,
 - f) lisensen.
2. En nærmere beskrivelse av elementene i modellen nevnt i nr. 1 og relevant informasjon om utviklingsprosessen, herunder
 - a) de tekniske midlene (for eksempel bruksanvisning, infrastruktur eller verktøy) som kreves for at KI-modellen for allmenne formål skal kunne integreres i KI-systemer,
 - b) konstruksjonsspesifikasjonene for modellen og treningsprosessen, herunder treningsmetoder og -teknikker, de viktigste konstruksjonsvalgene, inkludert begrunnelsen for dem samt de antakelsene som er gjort, hva modellen er konstruert for å optimere, og relevansen av de forskjellige parametrene, alt etter hva som er relevant,
 - c) informasjon om dataene som er brukt til trening, testing og validering, dersom det er relevant, herunder dataenes type og opprinnelse, kurateringsmetodene (for eksempel rensing eller filtrering), antall datapunkter og deres omfang og viktigste egenskaper, hvordan dataene er innhentet og valgt ut, samt alle andre tiltak for å påvise uegnede datakilder og metoder for å oppdage identifiserbare skjevheter, dersom det er relevant,
 - d) regnekraften som er brukt til å trene modellen (for eksempel antall flyttallsoperasjoner), treningstid og andre relevante detaljer om treningen,
 - e) kjent eller estimert energiforbruk for modellen.

Med hensyn til bokstav e) gjelder at dersom modellens energiforbruk er ukjent, kan energiforbruket baseres på informasjon om regnekraften som er brukt.

Avsnitt 2

Ytterligere opplysninger som skal gis av leverandører av KI-modeller for allmenne formål med systemrisiko

1. En detaljert beskrivelse av evalueringsstrategiene, herunder evalueringsresultater, på grunnlag av tilgjengelige offentlige evalueringsprotokoller og -verktøy eller andre evalueringsmetoder. Evalueringsstrategiene skal omfatte evalueringskriterier, mål og metoder for identifisering av begrensninger.
2. Dersom det er relevant, en detaljert beskrivelse av tiltakene som er iverksatt for å gjennomføre intern og/eller ekstern testing for ondsinnet bruk (for eksempel «red teaming») og modelltilpasninger, herunder innretting og finjustering.

3. Dersom det er relevant, en detaljert beskrivelse av systemarkitekturen som forklarer hvordan programvarekomponenter bygger på eller inngår i hverandre og er integrert i den samlede databehandlingen.

UOFFISIELL OVERSETTELSE

VEDLEGG XII

Opplysninger om åpenhet nevnt i artikkel 53 nr. 1 bokstav b) — teknisk dokumentasjon for leverandører av KI-modeller for allmenne formål til nedstrømsleverandører som integrerer modellen i sitt KI-system

Opplysningene nevnt i artikkel 53 nr. 1 bokstav b) skal minst omfatte følgende:

1. En generell beskrivelse av KI-modellen for allmenne formål, herunder
 - a) oppgavene som modellen er ment å utføre, og typen og arten av KI-systemer den kan integreres i,
 - b) de gjeldende retningslinjene for akseptabel bruk,
 - c) utgivelsesdatoen og distribusjonsmetodene,
 - d) hvordan KI-systemet samhandler med eller kan brukes til å samhandle med maskinvare eller programvare som ikke er en del av selve KI-systemet, dersom det er relevant,
 - e) versjonene av relevant programvare knyttet til bruken av KI-modellen for allmenne formål, dersom det er relevant,
 - f) arkitekturen og antallet parametere,
 - g) modaliteten (for eksempel tekst eller bilde) og formatet for inndata og utdata,
 - h) lisensen for modellen.
2. En beskrivelse av elementene i modellen og av prosessen for å utvikle den, herunder
 - a) de tekniske midlene (for eksempel bruksanvisning, infrastruktur eller verktøy) som kreves for at KI-modellen for allmenne formål skal kunne integreres i KI-systemer,
 - b) modaliteten (for eksempel tekst eller bilde) og formatet for inndata og utdata og deres maksimale størrelse (for eksempel kontekstvindusets lengde),
 - c) dersom det er relevant, informasjon om dataene som er brukt til trening, testing og validering, herunder dataenes type og opprinnelse samt kurateringsmetodene.

VEDLEGG XIII

Kriterier for utpeking av KI-modeller for allmenne formål med systemrisiko omhandlet i artikkel 51

For å fastslå at en KI-modell for allmenne formål har kapabiliteter eller en innvirkning tilsvarende det som er nevnt i artikkel 51 nr. 1 bokstav a), skal Kommisjonen ta hensyn til følgende kriterier:

- a) Antallet parametere i modellen.
- b) Kvaliteten eller størrelsen på datasettet, for eksempel målt ved hjelp av token.
- c) Datakraften som er brukt til å trene modellen, målt i antall flyttallsoperasjoner eller angitt med en kombinasjon av andre variabler, som estimerte treningskostnader, estimert nødvendig treningstid eller estimert energiforbruk til treningen.
- d) Inndata- og utdatamodalitetene i modellen, for eksempel tekst til tekst (store språkmodeller), tekst til bilde eller multimodalitet, og de nyeste tersklene for bestemmelse av kapabiliteter med høy påvirkningsgrad for hver modalitet, samt den spesifikke typen inndata og utdata (for eksempel biologiske sekvenser).
- e) Referanseverdier for og evalueringer av modellens kapabiliteter, herunder vurdering av antall oppgaver uten ytterligere trening, 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, hvilket skal antas å være tilfellet når den er gjort tilgjengelig for minst 10 000 registrerte bedriftsbrukere som er etablert i Unionen.
- g) Antall registrerte sluttbrukere.