Samspillet mellom AI Act og GDPR

Hvordan risikovurderingene som må foretas etter GDPR og AI Act samspiller og hvilke konsekvenser uklarheter og manglende harmonisering vil kunne få

Kandidatnummer: 33

Antall ord: 14825

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10.05.2023

Innholdsfortegnelse

1. Innledning

1.1 Tema og problemstilling

I februar 2023 uttalte Bill Gates at ChatGPT vil endre verden fundamentalt.[1] ChatGPT er en språkmodell og er kun ett eksempel på hvordan kunstig intelligens (heretter «KI») kan brukes. Den siste tiden har KI også blitt brukt til å generere kunst og Ukraina har brukt teknologien til å identifisere døde soldater.[2] For noen år siden var det utenkelig at KI kunne brukes på slike måter, men med en enorm utviklingshastighet øker mulighetene for hver dag som går. Dermed er det også umulig å forutse hvordan kunstig intelligens vil kunne brukes i fremtiden.

Selv om det ikke er tvil om at KI kan være nyttig, kan teknologien også utgjøre en stor risiko for menneskene som er utsatt for den. For å minimere risikoen forbundet med utvikling og bruk av KI, er det behov for rettslige avklaringer og begrensninger. Allerede i april 2018 uttalte Europakommisjonen (heretter «Kommisjonen») at det er behov for en koordinert tilnærming til utvikling og bruk av kunstig intelligens i EU. Dette er nødvendig for å få mest ut av mulighetene teknologien tilbyr, og for å møte de nye utfordringene som den medfører.[3] Videre uttalte de at EU bør være en pådriver av utviklingen for at den skal gagne alle og samtidig bygge på EU sine verdier og styrker.[4] På bakgrunn av dette ble det den 21. april 2021 lagt frem et forslag til en AI Act (heretter «Kommisjonens forslag»).[5] Forslaget har vært ute på offentlig høring og 6. desember 2022 publiserte Rådet for Den europeiske union (heretter «Rådet») et endringsforslag som er et kompromiss mellom de uttalte uenighetene som fremkom i den offentlige høringen (heretter «Rådets forslag»).[6]

---

[1] Rohan Goswami, «Bill Gates thinks A.I. like ChatGPT is the 'most important' innovation right now», *CNBC*, 10. februar 2023. [Tilgjengelig her: https://www.cnbc.com/2023/02/10/bill-gates-says-ai-like-chatgpt-is-the-most-important-innovation.html] (lest 17.03.2023).

[2] Xin Li, «Er dette fremtidens kunst?», *NRK*, 16. august 2022. [Tilgjengelig her: https://www.nrk.no/kultur/er-dette-fremtidens-kunst_-1.16048335]; John Birger Morud, «Ukraina bruker ansiktsgjenkjenning for å identifisere døde russiske soldater», *Forsvarets forum*, 4. april 2022. [Tilgjengelig her: https://forsvaretsforum.no/russland-ukraina/ukraina-bruker-ansiktsgjenkjenning-for-a-identifisere-dode-russiske-soldater/256609] (begge lest 24.04.2023).

[3] European Commission COM/2018/237 s. 2.

[4] Ibid.

[5] European Commission COM/2018/237; AI står for «artificial intelligence» og har samme betydning som KI på norsk.

[6] Council of EU, «Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights», pressemelding, 6. desember 2022. [Tilgjengelig her: Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights - Consilium (europa.eu)] (lest 17.3.2023).

AI Act er verdens første forslag til et juridisk rammeverk som regulerer KI spesifikt.[7] Når KI behandler personopplysninger innenfor EU eller om personer bosatt i EU, faller behandlingen imidlertid samtidig under personvernforordningen (heretter «GDPR»).[8] At automatisert behandling av personopplysninger ved bruk av KI faller inn under GDPR, fremgår av GDPR artikkel 4 nr. 2. Bestemmelsen definerer behandling av personopplysninger som «enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, **enten automatisert eller ikke**».[9] Når AI Act vedtas vil det følgelig være to regelverk som regulerer bruk av KI. Dette reiser spørsmål om samspillet mellom GDPR og fremtidens AI Act, og hvor godt regelverkene er harmonisert.

I Rådets forslag fortalepunkt 58a er det inntatt en generell presisering av forholdet til GDPR. Fortalepunktet presiserer for det første at forordningen ikke skal påvirke forpliktelsene til leverandører og brukere av KI-systemer i deres rolle som behandlingsansvarlige eller databehandlere etter GDPR. For det andre skal registrerte fortsette å nyte godt av alle rettighetene de har etter GDPR, inkludert rettighetene knyttet til automatiserte individuelle avgjørelser, herunder profilering etter GDPR art. 22. Videre fremgår det at harmoniserte regler for å utvikle, tilby og bruke KI-systemer under AI Act burde legge til rette for effektiv implementering og for andre rettigheter garantert av GDPR.

Utover denne overordnede presiseringen mangler det avklaringer av hvordan AI Act skal forholde seg til, og samspille med, GDPR i praksis. Oppgaven tar for seg en sentral problemstilling i forbindelse med dette. Denne problemstillingen er hvordan risikovurderingene i forslaget til AI Act samspiller med risikovurderingene som allerede må foretas etter GDPR. Det skal videre belyses hvilke konsekvenser eventuelle uklarheter og manglende harmonisering får for hovedaktørene under de to regelverkene.

1.2 Begrepsavklaringer

Verken GDPR eller AI Act har en legaldefinisjon av begrepet *risiko*. En naturlig språkforståelse tilsier at det må dreie seg om sannsynligheten for at et utfall får visse

[7] Digdir, «Ny forordning for kunstig intelligens», u.å. [Tilgjengelig her: *Ny forordning for kunstig intelligens*] (lest 07.03.2023).
[8] Europaparlamentets- 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) [GDPR]. Forordningen er gjennomført i norsk rett ved lov 20. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven) jf. personopplysningsloven § 1.
[9] Min utheving.

konsekvenser. Artikkel 29-gruppen (heretter «A29-gruppen») har videre definert risiko som et scenario som beskriver en hendelse og dens estimerte konsekvenser basert på alvorlighet og sannsynlighet.[10] En lignende definisjon er lagt til grunn av Datatilsynet som definerer risiko som «forholdet mellom sannsynligheten for at en uønsket hendelse vil inntreffe og konsekvenser av en slik hendelse.».[11]

Videre kan *risikohåndtering* defineres som samordnede aktiviteter som iverksettes for å styre og kontrollere en virksomhet basert på risiko.[12] Risiko kan med andre ord tjene som et utgangspunkt for beslutningstaking. Beslutninger tas på prognoser for fremtidige positive eller negative utfall. Disse vurderingene gjøres hovedsakelig gjennom praksis for risikoanalyser og risikostyring. Det vil si gjennom et sett med metoder, maler og prosesser ment å hjelpe til med å ta rasjonelle beslutninger.[13] Forslaget til AI Act er et tydelig eksempel på denne praksisen. KI-systemer skal kategoriseres innenfor fire ulike risikogrupper og det pålegges forskjellige forpliktelser til de ulike aktørene avhengig av risikogruppen systemet faller innunder.[14] På denne måten definerer forordningen direkte evaluering av risiko og hvilke avbøtende tiltak som må iversettes fra et *ovenfra-og-ned perspektiv*.

GDPR er også en risikobasert rettsakt. Dette kan forankres allerede i et av de grunnleggende prinsippene for behandling av personopplysninger, ansvarlighetsprinsippet, men fremgår også av GDPR artikkel 24, 32 mfl.[15] Ansvarlighetsprinsippet presiseres i GDPR artikkel 5 nr. 2 som sier at «[d]en behandlingsansvarlige er ansvarlig for og skal kunne påvise at [de øvrige personvernprinsippene] overholdes».

At behandlingsansvarlige har en slik forpliktelse kan tolkes som et ansvar for risikostyring. Behandlingsansvarliges aktiviteter skal gjøres for å minimere risiko i tråd med forpliktelsene etter GDPR.[16] Dersom ansvarlighetsprinsippet forstås på denne måten, vil hele GDPR ha en

---

[10] A29-gruppen, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679*, veileder, 4. april 2017, WP 248, s. 6. Oversettelsen er tatt fra den uoffisielle norske versjonen 17/00282-1.
[11] Datatilsynet, «Informasjonssikkerhet og internkontroll: Risikovurdering», sist endret 16.07.2019 (sitert 15.03.2023).
[12] A29-gruppen, DPIA-retningslinje, s. 6.
[13] Giovanni De Gregorio og Pietro Dunn. «The European Risk-based Approaches: Connecting Constitutional Dots in the Digital Age», *Common Market Law Review 59*, 2 (2022), s. 473-500, på s. 3. [DOI: https://dx.doi.org/10.2139/ssrn.4071437] (lest 10.3.2023).
[14] Se punkt 4.2.
[15] Raphaël Gellert, *The risk-based approach to data protection*, 1. utgave, Oxford University Press, 2020 s. 138.
[16] Ibid.

risikobasert tilnærming og ikke bare de artikklene som oppstiller konkrete krav til å foreta risikovurderinger. Disse behandles nærmere i punkt 5.2 og 5.3.

Denne formen for risikostyring følger et *nedenfra-og-opp*-perspektiv og ikke et slikt *ovenfra-og-ned*-perspektiv som i AI Act.[17] Med dette menes at i GDPR er evalueringen av risiko og valg av avbøtende tiltak ikke definert av loven, fra et ovenfra-og-ned perspektiv, men først og fremst overlatt til behandlingsansvarliges skjønn. GDPR legger opp til at det er behandlingsansvarlige som er nærmest å vurdere risikoen og iverksette risikoreduserende tiltak. Det er behandlingsansvarlig som kjenner behandlingen best, og egen ressurssituasjon, og dermed har forutsetning for å vurdere hvilke tiltak som vil virke best. Lovteksten bestemmer ikke hvilke tiltak som skal iverksettes, men lister opp noen som skal vurderes. En slik *nedenfra-og-opp* regulering er resultatet av en lovgivningsstrategi som tar sikte på å redusere forpliktelser som kommer *ovenfra*.[18]

1.3 Rettskilder og metodiske utfordringer

Personvern er en av de grunnleggende rettighetene nedfelt i EUs primærrett. Rettigheten fremgår av artikkel 8 nr. 1 i Den europeiske unions pakt om grunnleggende rettigheter[19] og artikkel 16 nr. 1 i traktaten om Den europeiske unions virkemåte (TEUV).[20] Etter TEUV artikkel 16. nr. 2 har Europaparlamentet (heretter «Parlamentet») og Rådet videre fullmakt til å fastsette regler om vern av fysiske personer i forbindelse med behandling av personopplysninger. Det er disse bestemmelsene som utgjør hjemmelsgrunnlaget både for GDPR og for de delene av AI Act som omhandler personopplysninger.[21] AI Act for øvrig er hjemlet i TEUV artikkel 114 som omhandler det indre marked i EU sin funksjon og harmonisering av medlemsstatenes lovgivning i tråd med denne.[22] Når AI Act vedtas utgjør både GDPR og AI Act etter dette sekundærlovgivning i EU. De bygger på de politiske målene og rettighetene som fremgår av EUs primærrett.[23]

GDPR trådte i kraft 25. mai 2018. At GDPR er en forordning medfører at den er allmenngyldig og gjelder direkte for EUs medlemsland fra og med tidspunktet den trer i kraft jf. TEUV artikkel 288(2). Forordningen gjelder også for Norge gjennom EØS-avtalen, men i

[17] De Gregorio og Dunn (2022) s. 4.
[18] Ibid.
[19] Charter of Fundamental Rights of the European Union 2000/C 364/01.
[20] Consolidated version of the Treaty on the Functioning of the European Union 2012/C 326/01.
[21] GDPR fortalepunkt 12; Rådets forslag fortalepunkt 2.
[22] Ibid.
[23] Odd Stemsrud, *EØS-rett i et nøtteskall*, 1. utgave, Gyldendal 2016, s. 69.

motsetning til i EU-medlemslandene måtte den gjennomføres i norsk lov først.[24] Selv om GDPR gjelder ord for ord, åpner forordningen selv for nasjonale tilpasninger. Eksempelvis er det flere av kravene i kapittel IV som gjelder med mindre noe annet kreves i henhold til nasjonal rett.[25]

Når AI Act vedtas vil den også være en forordning. I og med at regelverket foreløpig kun er et forslag er det nødvendig i korte trekk å forklare beslutningsprosessen frem til den får anvendelse i EØS.

Den ordinære regelverksprosessen i EU er forankret i TEUV artikkel 294 og består av flere trinn som involverer ulike aktører på ulike nivåer i EU. Det er Kommisjonen som legger frem forslag til nye forordninger.[26] Disse legges frem i COM-dokumenter.[27] Selv om Kommisjonen formelt har initiativretten til å foreslå nye forordninger, avhenger hvilke forordninger som foreslås og innenfor hvilke felt, av hva som står på den politiske dagsordenen i EU å regulere.[28] Etter at Kommisjonen har publisert sitt forslag er det Parlamentet og Rådet sammen som skal vedta forordningen og må bli enige om den endelige teksten. Prosessen frem mot dette kan foregå på litt ulike måter. Det vil også variere fra rettsakt til rettsakt hvor mange behandlinger som kreves.[29]

Prosessen frem mot endelig AI Act har foreløpig foregått ved at Kommisjonens kom til enighet om et forslag og stemte over dette. Deretter ble det offentliggjort i EURLEX og kunngjort i en pressemelding 21. april 2021.[30] Etter dette har det vært ute på offentlig høring. I Parlamentet er prosessen ledet av to komiteer, Committee on Internal Market and Consumer Protection (IMCO) og Committee on Civil Liberties, Justice and Home Affairs (LIBE), som i løpet av 2022 foreslo endringer.[31] Ytterligere fem andre komiteer må imidlertid også tas til

[24] Se personopplysningsloven § 1.
[25] Se for eksempel GDPR art. 29 og 32 nr. 4.
[26] TEUV art. 294 nr. 2.
[27] Utenriksdepartementet, «Slik blir EØS-regelverk til», 21. mars 2023. [Tilgjengelig her: https://www.regjeringen.no/no/tema/europapolitikk/eos1/eos-regelverk/id686837/] (lest 28.03.2023).
[28] Ibid.
[29] Ibid.
[30] European Commission, «Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence», pressemelding, 21. april 2021. [Tilgjengelig her: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682] (lest 28.03.2023).
[31] European Parliament, «Proposal for a Regulation on a European approach for Artificial Intelligence», *A Europe Fit for the Digital Age*, Legislative train, 20. mars 2023. [Tilgjengelig her: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence] (lest 08.04.2023).

etterretning i arbeidet med endelig tekst.[32] Basert på de offentliggjorte høringsinnspillene, både fra medlemsland, private aktører og Parlamentets komiteer, publiserte Rådet den 6. desember 2022 en pressemelding med sitt endringsforslag.[33] I løpet av semestret denne oppgaven skrives har Kommisjonen og Rådet ventet på Parlamentets endelige holdning. Den 27. april uttalte Parlamentets medlemmer (MEPs) at de har kommet til enighet, men at det gjenstår å skrive ut teksten.[34] Når Parlamenters holdning og forslag publiseres skal partene gå inn i «trilog»-forhandlinger (Trilogue negotiations).[35] Endelig forordningsvedtak er ventet i slutten av 2023 eller starten av 2024.

Når AI Act vedtas i EU er den gjeldende i alle EUs medlemsland slik som GDPR, men det skal en ytterligere prosess til før den trer i kraft her i Norge. Før en forordning trer i kraft i EØS, må den innlemmes i EØS-avtalen.[36] Vanligvis foregår dette ved at EØS-komiteen bestående av representanter fra EU og EØS/EFTA-landene (Norge, Island og Liechtenstein)[37] fatter beslutning om innlemmelse i EØS avtalen og enes om hvordan dette skal gjøres.[38] Forordninger skal etter EØS-avtalen artikkel 7 gjennomføres «som sådan».[39] Dette innebærer at de skal innlemmes i sin helhet som et vedlegg i EØS-avtalen. Deretter må EØS-landene oftest gjøre endringer i sin nasjonale lovgivning for å gjennomføre forordningen. Et eksempel er personopplysningsloven § 1 som gjennomfører GDPR i norsk lov. Først når forordningen er innlemmet i EØS-avtalen og gjennomført i nasjonal lov, vil den få samme rettslige virkning i EØS/EFTA-landene som den har for EU medlemslandene.[40]

---

[32] Jonas Schuett, «Risk Management in the Artificial Intelligence Act», *European Journal of Risk Regulation*, First View (2023), s. 1-19, på s. 4. [DOI: https://doi.org/10.1017/err.2023.1] (lest 03.05.2023).
[33] Council of EU, «Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights», pressemelding, 6. desember 2022.
[34] Luca Bertuzzi, «MEPs seal the deal on Artificial Intelligence Act», *Euractive*, 27. april 2023, oppdatert 28. april 2023. [Tilgjengelig her: https://www.euractiv.com/section/artificial-intelligence/news/meps-seal-the-deal-on-artificial-intelligence-act/] (lest 03.05.2023).
[35] Trilog-forhandlinger er uformelle forhandlinger om lovforslag mellom representanter for Parlamentet, Rådet og Kommisjonen. Formålet er å oppnå en enighet mellom Parlamentet og Rådet om en lovtekst. Parlamentet har skrevet om disse på sine sider: Interinstitutional negotiations | Ordinary Legislative Procedure | European Parliament (europa.eu) (lest 28.03.2023).
[36] Utenriksdepartementet, «Slik blir EØS-regelverk til», 21. mars 2023.
[37] Sveits er også et EFTA-land, men er ikke med i EØS avtalen.
[38] Utenriksdepartementet, «Slik blir EØS-regelverk til», 21. mars 2023.
[39] The Agreement on the European Economic Area, Porto, 1992 (EØS-avtalen).
[40] Ibid.

Da Kommisjonens forslag til AI Act ble publisert ble den ikke markert som EØS-relevant.[41] I følge Kommunal- og distriktsdepartementet er dette trolig en uteglemmelse. Dersom forordningen vedtas, er det sannsynlig at AI Act har EØS-relevans og må tas inn EØS-avtalen.[42]

Selv om AI Act kun er et forslag, kommer jeg til å legge EUs tolkningsprinsipper til grunn på samme måte som når GDPR tolkes. EUs tolkningsprinsipper er utviklet gjennom rettspraksis fra EU-domstolen. I likhet med norsk rettskildelære tas utgangspunktet i ordlyden til de enkelte bestemmelsene.[43] Dersom ordlyden i en språkversjon åpner for uklarheter, kan sammenligning med ordlyden i andre av de 24 offisielle språkversjonene bidra til klarhet.[44] Når oppgaven behandler GDPR kommer jeg, av praktiske hensyn, til å bruke den norske oversettelsen gjennomført i norsk lov ved personopplysningsloven § 1. Den norske språkversjonen er ikke en offisiell språkversjon innenfor EU. Dermed vil det vises til offisielle språkversjoner dersom den norske ordlyden ikke er klar eller gir rom for flere tolkningsalternativer. Derimot vil de engelske versjonene av forslagene til AI Act benyttes da det ikke finnes offisielle norske oversettelser.

Kontekst og formål får videre stor vekt når ordlyden i de enkelte bestemmelsene tolkes.[45] Dette kan begrunnes i grunnforutsetningen om en autonom og ensartet tolkning av EU-retten.[46] Der de offesielle språkversjonene gir uttrykk for ulike språklige nyanser, kan kontest og formål ofte bidra til å belyse hva innholdet i en bestemmelse er. Fortalene til forordninger er ikke rettslig bindende, men utgjør en del av konteksten og kommer derfor til å benyttes aktivt i oppgaven.[47]

Forarbeider har derimot ikke den samme vekten i EU som i Norge. Disse kan anvendes til å kontekstuelt avkrefte eller bekrefte ulike tolkningsalternativer. De kan også brukes til å illustrere lovgivningsprosessen, men som hovedregel ikke til mer.[48] De foreløpig publiserte versjonene av AI Act vil regnes som forarbeider sett i lys av den endelige versjonen som

---

[41] Kommunal- og distriktsdepartementet, «Forslag til forordning om kunstig intelligens (KI-forordningen)». EØS-notat, 21. juni 2021, sist oppdatert 12. november 2021. [Tilgjengelig her: Forslag til forordning om kunstig intelligens (KI-forordningen) - regjeringen.no] (sitert 11.03.2023).
[42] Ibid.
[43] Se for eksempel *OT v Vyriausioji tarnybinės etikos komisija* [GC] C-184/20, avsnitt 121.
[44] Se for eksempel European Union, «Languages», på EU sin hjemmeside. [Tilgjengelig her: https://european-union.europa.eu/principles-countries-history/languages_en] (lest 19.04.2023).
[45] *OT v Vyriausioji tarnybinės etikos komisija* [GC] C-184/20, avsnitt 121.
[46] Fredriksen og Mathisen (2018) s. 295.
[47] Fredriksen og Mathisen (2018) s. 305.
[48] Fredriksen og Mathisen (2018) s. 306.

vedtas etter at denne oppgaven er publisert. Samtidig indikerer diskusjonene og de tekniske møtene avholdt i EU første halvdel av 2023 at Rådets forslag ligget relativt nært det som blir den endelig vedtatte teksten og det ansees dermed trygt å ta utgangspunkt i denne.[49] Selv om det ansees som trygt, vil utgangspunktet og hovedvekten ligge på GDPR. Det som skal vurderes er hvordan risikovurderingene i forslaget til AI Act vil samspille med den allerede vedtatte GDPR. Dette vil bidra til å fremme hvordan de to regelverkene bør praktiseres og samspille med hverandre i fremtiden.

EU-domstolens avgjørelser er også sentrale tolkningsbidrag i den EU-rettslige metoden.[50] Det er imidlertid ingen avgjørelser som belyser samspillet mellom AI Act og GDPR. Dette skyldes at AI Act ikke er vedtatt. Når AI Act trer i kraft er det EU-domstolens oppgave å tolke bestemmelsene, oppklare uklarheter og å avgjøre tvister. Gjennom TEU artikkel 19 nr. 1 er domstolen tillagt betydelig makt som unionens øverste vokter.[51] Den er også gitt omfattende, eksklusiv og obligatorisk jurisdiksjon til å tolke EU-retten og å avgjøre tvister. Dermed utgjør den en autoritativ rettskilde i EU-rettslig forstand.[52]

Det er etter hvert mye juridisk litteratur som omhandler GDPR og den risikobaserte tilnærmingen, inkludert de konkrete risikovurderingene som må foretas. Derimot er det lite juridisk litteratur om forslaget til AI Act og jeg har kun klart å identifisere én artikkel som sammenligner de risikobaserte tilnærmingene i begge. I lys av det tynne rettskildebilde og mangelen på autoritative rettskilder som behandler oppgavens problemstilling, vil den juridiske litteraturen anvendes som tolkningsbidrag og få relativt stor vekt i analysen. Karnov-kommentarene til personvernforordningen vil også vises til.

Videre er uttalelser, veiledninger og retningslinjer fra European Data Protection Board (heretter «EDPB») viktige. EDPB er opprettet i medhold av GDPR artikkel 68 nr. 1. Uttalelsene er ikke juridisk bindende, men bør tillegges stor vekt da kompetansen deres er hjemlet direkte i GDPR. EDPB ble etablert 25. mai 2018 og har som hovedoppgave å «sikre ensartet anvendelse av [...] forordning[en]» jf. GDPR artikkel 70 nr. 1. Før etableringen av EDPB var det A29-gruppen som var EUs rådgivende organ i personvernspørsmål.

[49] Mer om hvorfor denne versjonen brukes og hvorfor det ansees trygt under punkt 1.4.1.
[50] Fredriksen og Mathisen (2018) s. 317.
[51] Fredriksen og Mathisen (2018) s. 153.
[52] Ibid.

På EDPB sitt første møte ga de sin tilslutning til A29-gruppen sine veiledninger.[53] Disse har følgelig fortsatt rettskildemessig vekt i relasjon til GDPR.

Til slutt vil det vises til artikler, veiledninger og uttalelser fra Datatilsynet og andre statlige organer. Disse har ikke autoritativ vekt, men har stor reell og praktisk betydning. De bidrar til å belyse hvordan Norge har valgt å tolke GDPR. Videre er de informative om tematikken rundt kunstig intelligens og toneangivende for å belyse Norges posisjon i debatten om fremtidens regulering.

1.4 Avgrensninger og fremstillingen videre

1.4.1 Avgrensninger

Problemstillingen omhandler kun den risikobaserte tilnærmingen i forslaget til AI Act og GDPR og hvilke risikovurderinger hovedaktørene må foreta. Det avgrenses mot andre tilfeller av manglende harmonisering mellom regelverkene. Dette inkluderer kravene til å varsle myndigheter og registrerte[54], kravene til transparens og åpenhet[55], systemene for sertifisering/sertifikater[56] og reglene for sanksjoner.[57] Likevel vil det noen steder kommenteres at det foreligger avvik.

Begrepet «hovedaktørene» viser til behandlingsansvarlig og databehandler under GDPR.[58] Under AI Act vises det til leverandører og brukere.[59] Det er disse aktørene som er hovedfokuset i oppgaven. Andre viktige aktører, slik som den registrerte etter GDPR artikkel 4 nr. 1, vil likevel nevnes der det er nødvendig.

Videre tar denne oppgaven utgangspunkt i Rådets forslag fra 6. desember 2022 da dette var den nyeste versjonen av forslaget per Q1 2023. Parlamentets endelige forslag var opprinnelig ventet i slutten av mars 2023, men først 27. april ble det bekreftet at de hadde kommet til enighet.[60]

---

[53] EDPB, «Endorsed WP29 Guidelines», på EDPB sin hjemmeside. [Tilgjengelig her: https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en] (lest 04.04.2023).
[54] GDPR art. 33 og 34 og Rådets forslag art. 22, 32 og 62.
[55] GDPR art. 5 nr. 1, 12, 13 og 14 og Rådets forslag art. 52.
[56] GDPR art. 42 og 43 og Rådets forslag art. 44.
[57] GDPR art. 84 og Rådets forslag art. 71. Dersom aktørene risikerer å sansksjoneres både etter GDPR og AI Act for samme forhold, kan det bryte med andre viktige prinsipper.
[58] GDPR art. 4 nr. 7 og 8, se oppgavens punkt 3.3.
[59] AI Act art. 3 nr. 2 og 6, se oppgavens punkt 4.1.
[60] Luca Bertuzzi, «MEPs seal the deal on Artificial Intelligence Act», *Euractive*, 27. april 2023, oppdatert 28. april 2023.

Parliamentet har fortsatt annledning til å gjøre mindre tekniske endringer i teksten og den vil ikke publiseres før den er stemt over i komiteene 11. mai og i plenum i Parlamentet i midten av juni 2023.[61] Selv om teksten ikke er publisert har det i løpet av vårsemestret 2023 blitt avholdt en rekke tekniske møter som indikerer hvilke endringer Parlamentet kommer til å foreslå.[62] Det vil for det første ilegges strengere krav for språkmodeller som ChatGPT. Det er blant annet debatten rundt hvordan disse modellene skal reguleres som har forsinket lovgivningsprosessen.[63] Videre har listene over både forbudte KI-systemer og høyrisiko KI-systemer blitt utvidet. Til sist, og av særlig relevans for denne oppgaven, har Parlamentet kommet til enighet om flere endringer i leverandørers krav til risikostyring.[64] I Kommisjonens og Rådets forslag skal KI-systemer listet opp i vedlegg III til forordningen automatisk regnes som høyrisiko.[65] Etter Parlamentets forslag må det derimot foretas en ytterligere risikovurdering av om disse systemene utgjør en betydelig risiko for helse, sikkerhet eller EUs grunnleggende rettigheter. Først da regnes KI-systemene som høyrisiko.[66] Det er også ilagt strengere krav til transparens og journalføring. For brukere av KI-systemer er det ilagt krav om å foreta en konsekvensanalyse for å vurdere potensiell innvirkning på de grunnleggende rettighetene til fysiske personer som er berørt av systemet.[67]

I og med at Parlamentets forslag til tekst ikke er publisert når oppgaven leveres er det videre kun teksten i Rådets forslag og Kommisjonens forslag det skal vises til. Denne oppgaven er en rettsdogmatisk analyse av kildene som er tilgjengelig på tidspunktet oppgaven skrives og endringer publisert etter 30. april 2023 må det avgrenses mot.

Selv om oppgaven ikke vurderer Parlamentets forslag er det imidlertid svært sannsynlig at analysen vil være relevant for forståelsen av det fremtidige rettskildebildet. På tross av de nevnte endringene, er det ingen indikasjoner på andre endringer av stor betydning.[68]

---

[61] Ibid.
[62] Ibid.
[63] Luca Bertuzzi, «AI Act: European Parliament headed for key committee vote at end of April», *Euractive*, 30. mars 2023, oppdatert 31. mars 2023. [Tilgjengelig her: https://www.euractiv.com/section/artificial-intelligence/news/ai-act-european-parliament-headed-for-key-committee-vote-at-end-of-april/] (lest 08.04.2023).
[64] Ibid.
[65] Se oppgavens punkt 4.2.2 om dette.
[66] Luca Bertuzzi, «MEPs seal the deal on Artificial Intelligence Act», *Euractive*, 27. april 2023, oppdatert 28. april 2023.
[67] Ibid.
[68] Schuett (2023) s. 4.

Den risikobaserte tilnærmingen og systemet i forslaget for øvrig er det enighet om, herunder hovedlinjene i artikkel 9, som er særlig viktig for denne oppgaven.[69]

Når begrepene «AI Act» eller «AIA» brukes, vises det til forslaget til KI-forordning generelt. Med andre ord brukes disse begrepene der det ikke er nødvendig å påpeke om det er tale som Kommisjonens eller Rådets forslag. Selv om oppgaven tar utgangspunkt i Rådets forslag, vil det vises til Kommisjonens forslag der det er nødvendig for å belyse ulike tolkningsalternativer eller utviklingen.

1.4.2 Fremstillingen videre

Oppgaven starter med å definere kunstig intelligens i kapittel 2. I kapittel 3 presenteres hovedaktørene under GDPR og de prinsippene for behandling av personopplysninger som er relevante i lys av problemstillingen. I kapittel 4 presenteres AI Act. Det redegjøres først for hovedaktørene under AI Act for å identifisere hvilken rolle disse har under GDPR. Deretter presenteres systemet i forslaget, inkludert den risikobaserte tilnærmingen.

I kapittel 5 sammenlignes de risikobaserte tilnærmingene i AI Act og GDPR, inkludert konkrete bestemmelser som oppstiller krav til risikovurderinger i de to regelverkene. Deretter redegjøres det for konsekvensene av uklarheter og manglende harmonisering.

I del 6 sammenstilles funnene gjort i den rettsdogmatiske analysen. Basert på disse funnene vil det trekkes frem noen betrakninger på hvordan konsekvensene kan begrenses, de lege ferenda.

[69] Ibid.

2. Kunstig intelligens (KI)

For den videre fremstillingen er det nødvendig å definere begrepet kunstig intelligens. Dette er viktig fordi oppgaven kun tar for seg de situasjonene der kunstig intelligens behandler personopplysninger på en slik måte at bruken faller inn under både AIA og GDPR.

2.1 Definisjoner

Det finnes en rekke ulike definisjoner av KI og KI-systemer. Hva som menes med KI varierer også noe mellom tekniske felt, juridiske felt og hvordan begrepet brukes i dagligtalen. I dagligtalen brukes kunstig intelligens og maskinlæring ofte synonymt, selv om dette er upresist.[70] Definisjonen som har relevans i denne oppgaven er den som skal anvendes i AI Act og som dermed vil bestemme anvendelsesområdet til den fremtidige forordningen.

I artikkel 3 nr. 1 i Rådets forslag er et KI-system definert som:

> *[A] system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts.*

Definisjonen i Rådets forslag er snevrere enn i Kommisjonens opprinnelige forslag. I tillegg til «machine learning approaches» og «logic- and knowledge-based approaches», gjalt Kommisjonens forslag «statistical approaches».[71] Dette skapte stor debatt og en rekke medlemsland og store internasjonale organisasjoner uttrykte misnøye. I mai 2019 kom OECD med sin posisjon til forslaget hvor de avgrenser definisjonen til å kun gjelde maskinlæringssystemer.[72] I et møte den 3. mars 2023 kom de politiske gruppene som jobber med AI Act i Parlamentet til enighet.[73] Selve teksten er ikke ferdigstilt, men er i stor grad i tråd med OECD sin definisjon. Teksten de diskuterte var:

---

[70] Datatilsynet, «Kunstig intelligens og personvern», rapport, 11. januar 2018, s. 5.
[71] European Commission COM/2021/206 art. 3 nr. 1 s. 39.
[72] OECD, *Recommendation of the Council on Artificial Intelligence*, 22. mai 2019, OECD/LEGAL/0449.
[73] Luca Bertuzzi, «EU lawmakers set to settle on OECD definition for Artificial Intelligence», *Euractive*, 7. mars 2023, oppdatert 9. mars 2023. [Tilgjengelig her: EU lawmakers set to settle on OECD definition for Artificial Intelligence – EURACTIV.com] (lest 10.04.2023).

> *Artificial intelligence system' (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate output such as predictions, recommendations, or decisions influencing physical or virtual environments.*[74]

Parlamentet kom imidlertid frem til at «machine-based systems» skal fjernes slik at den favner litt videre og det skal sørges for at modeller som ChatGPT ikke faller gjennom.[75]

Selv om Parlamentets forslag til tekst ikke er publisert og forordningen ikke er vedtatt, er det sterke indikasjoner på at endelig definisjon vil være i tråd med dette. Den videre lovgivningsprosessen og trilog-forhandlingene avhenger av at AIAs anvendelsesområde i det minste er avklart. Derfor legges denne definisjonen til grunn videre i oppgaven.

2.2 Maskinlæringssystemer

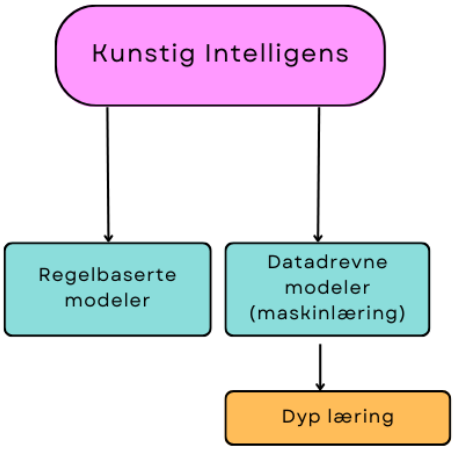
Selv om AI Act ikke bare skal regulere maskinlæsingssystemer, er det disse systemene som i størst grad vil utgjøre en risiko for mennesker som er utsatt for dem. Et maskinlæringssystem er en form for KI-system, men KI omfatter også andre enklere systemer slik som regelbaserte modeller.

Maskinlæring er teknikker og verktøy som brukes til å lage matematiske algoritmer basert på innsamlet data.[76] Et maskinlæringssystem vil kunne videreutvikle seg selv uten nye menneskelige bidrag. Systemet vil også kunne bygge nye algoritmer. Desto mer ny og ulik type data systemet eksponeres for, desto mer lærer det. Dermed genererer det kunnskap fortløpende samtidig som systemet blir mer treffsikkert og kan gi bedre svar jo mer data det eksponeres for.[77]

En form for et maskinlæringssystem er *dyp læring*. Dyplæringssystemer tar utgangspunkt i et kjent treningsdatasett, men klarer deretter å finne løsningen på egen hånd.[78] På samme måte som hjernen kan lære å gjenkjenne mønstre og sammenhenger gjennom erfaring, kan dyp læring lære å gjøre prediksjoner og ta beslutninger basert på store mengder data.[79]

---

[74] Ibid.
[75] Ibid.
[76] Datatilsynet, «Kunstig intelligens og personvern», rapport, 11. januar 2018, s. 5.
[77] Ibid.
[78] Datatilsynet, «Kunstig intelligens og personvern», rapport, 11. januar 2018, s. 12.
[79] Ibid.



Figur 1: forenklet illustrasjon av forholdet mellom KI, maskinlæring og dyp læring[80]

Det er særlig tre problemstillinger bruk av makinlæring reiser i relasjon til GDPR. For det første er det behov for relativt store mengder treningsdata for at modellene skal bli funksjonelle og virke til sin hensikt. Dette kan være problematisk sett i lys av dataminimeringsprinsippet i GDPR.[81] For det andre må dataen også være betydningsfull og korrekt. Mangel på korrekt eller betydningsfull data kan medføre forutinntatthet og diskriminering i modellene.[82] Dette kan være problematisk i henhold til blant annet rettferdighetsprinsippet ettersom diskriminering i modellene kan medføre urettmessig forskjellsbehandling.[83] For det tredje kan modellene bli såpass komplekse og avanserte at de endelige resultatene vanskelig lar seg forklare. Det vil være utfordrende å ettergå resultatene og å finne ut hvilke data som var nødvendig for utfallet.[84] Dette kan være problematisk sett i lys av åpenhetsprinsippet.[85] Disse utfordringene behandles nærmere under gjennomgangen av personvernprinsippene i punkt 3.3.

[80] Min egen fremstilling.
[81] GDPR art. 5 nr. 1 bokstav c.
[82] Ignacio N. Cofone, «Algorithmic Discrimination Is an Information Problem», *Hastings Law Journal 70*, 6 (2019) s. 1389-1444, på s. 5. [Tilgjengelig her: https://www.hastingslawjournal.org/algorithmic-discrimination-is-an-information-problem/] (lest 14.03.2023).
[83] GDPR art. 5 nr. 1 bokstav a.
[84] Datatilsynet, «Kunstig intelligens og personvern», rapport, 11. januar 2018, s. 12.
[85] GDPR art. 5 nr. 1 bokstav a. Det kan også gjøre det vanskelig å overholde den registrertes rett til informasjon etter GDPR art. 13 og 14 og retten til innsyn etter GDPR art. 15.

3. GDPR - Nåværende regulering av kunstig intelligens

Ovenfor har jeg definert KI-systemer. For å besvare oppgavens problemstilling må det vurderes hvordan disse systemene reguleres etter GDPR idag. I det følgende skal det først gis et kort overblikk over GDPR, herunder formålet, hva som menes med personopplysninger og hvilke typer personopplysninger forordningen skiller ut. Videre skal det gjøres rede for de personvernprinsippene som har særlig relevans når personopplysninger behandles av KI-systemer. Dette gjøres i punkt 3.3. Deretter skal det gjøres rede for hovedaktørene under GDPR med hovedfokus på behandlingsansvarlig og databehandler. Det er disse det skal tas utgangspunkt i når oppgaven under punkt 4.1 kartlegger hvem som er leverandør og bruker under AI Act.

3.1 Et overblikk

GDPR har to hovedformål som fremgår av artikkel 1 nr. 1.[86] For det første skal forordningen sikre «vern av fysiske personer i forbindelse med behandling av personopplysninger» og for det andre skal forordningen sikre «fri utveksling av personopplysninger». GDPR har derfor som formål å verne fysiske individer, uavhengig av om behandlingen av personopplysninger er gjort av fysiske mennesker eller ved hjelp av teknologi som kunstig intelligens. At teknologi som kunstig intelligens omfattes fremkommer også av definisjonen av «behandling» av personopplysninger presentert under punkt 1.2.

Videre er personopplysninger definert i GDPR artikkel 4 nr. 1 som «enhver opplysning om en identifisert eller identifiserbar fysisk person». Disse typene personopplysninger vil tiltales som alminnelige personopplysninger.[87] Ved siden av alminnelige personopplysninger, skiller GDPR ut to sensitive kategorier av personopplysninger. Dette er særlige kategorier av personopplysninger jf. GDPR artikkel 9 nr. 1 og personopplysninger om straffedommer og lovovertredelser jf. GDPR artikkel 10. Behandling av disse typene personopplysninger kan utgjøre en risiko for personers grunnleggende rettigheter og friheter og krever derfor særskilt vern.[88] Når risikoen for den registrerte øker krever GDPR også at det må foretas ytterligere

[86] Se også GDPR fortalepunkt 3.
[87] Denne termen ble introdusert av Dag Wiese Schartum. Se Dag Wiese Schartum, *Personvernforordningen – en lærebok*, 1. utgave, Fagbokforlaget, 2020, s. 46.
[88] GDPR art. 9 nr. 1.

risikovurderinger, en DPIA, før behandlingen kan starte. Dette kommer jeg tilbake til under punkt 5.2.

Det er videre en bevvist strategi at forordningen er teknologinøytral. Dette er gjort for å unngå risikoen for at vernet forordningen gir fysiske personer kan omgås.[89] AIA er til sammenligning, ikke teknologinøytral. GDPR har et vidt virkeområde, mens AIA gir særreguleringer for én type teknologi (kunstig intelligens). En annen viktig forskjell er at GDPR gir rettigheter til enkeltindivider. AIA gjør ikke dette, selv om forslaget også i praksis vil verne enkeltindivider.

3.2 Hovedaktørene under GDPR

Aktørene som er involvert i behandlingen av personopplysninger er *behandlingsansvarlig, databehandler og den registrerte*. De fleste forpliktelsene etter GDPR pålegges den **behandlingsansvarlige**.[90] Det er behandlingsansvarlig som er ansvarlig for risikoen og som må gjennomføre de fleste risikovurderingene etter GDPR.[91] Behandlingsansvarlig er definert som:

> *[E]n fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; [...].*[92]

Behandlingsansvarlig er følgelig den som bestemmer formålet med en behandling og hvilke hjelpemidler, eksempelvis kunstig intelligens, som skal brukes.[93] Behandlingsansvarlig trenger imidlertid ikke være den som utfører selve behandlingen. En **databehandler** er en som behandler personopplysninger på vegne av behandlingsansvarlige. Databehandlere er definert som:

> *[E]n fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.*[94]

Den registrerte er den identifiserte eller identifiserbare fysiske personen det behandles personopplysninger om som har rettigheter etter GDPR.[95]

[89] GDPR fortalepunkt 15.
[90] NOU 2022: 11 Ditt personvern – vårt felles ansvar. Tid for en personvernpolitikk, s. 38.
[91] Se oppgavens punkt 5.
[92] GDPR art. 4 nr. 7.
[93] NOU 2022: 11 s. 38.
[94] GDPR art. 4 nr. 8.
[95] GDPR art. 4 nr. 1.

Som jeg kommer tilbake til under punkt 4.1 og 5.3.1 vil rollefordelingen mellom aktørene under GDPR og AI Act endre seg gjennom livsløpet til en KI eller for ulike deler av behandlingen. Dette kan få konsekvenser når risikovurderinger etter begge regelverk skal foretas.

3.3 Prinsipper for behandling av personopplysninger med bruk av KI

Personvernprinsippene fremgår av GDPR artikkel 5 og kan sees på som grunn-normer som gir generelle, overordnede retningslinjer for hva som må vektlegges for å ivareta personvernet.[96] Samtidig utgjør de positive rettigheter som registrerte kan påberope seg og som behandlingsansvarlig kan sanksjoneres for brudd på. Dette kommer til uttrykk av ansvarlighetsprinsippet etter GDPR artikkel 5 nr. 2. Bestemmelsen pålegger behandlingsansvarlig en positiv plikt til overholdelse av personvernprinsippene og til å påvise overholdelsen.

Selv om alle personvernprisippene er veiledende ved all form for behandling av personopplysninger, ansees noen særlig utfordrende i lys av problemstillingen. Dette er for det første ansvarlighetsprinsippet gjennomgått overnfor. Dette gir både uttrykk for den risikobaserte tilnærmingen i GDPR og forankrer at behandlingsansvarlig er ansvarlig for risikoen i GDPR.[97] Videre har Datatilsynet i sin rapport om kunstig intelligens og personvern trukket frem prinsippene om åpenhet/gjennomsiktighet, rettferdighet, formålsbegrensning og dataminimering.[98] Det er disse prinsippene som i korte trekk skal presenteres og hvor relevansen til oppgavne skal trekkes frem.

3.3.1 Rettferdighet og åpenhet

Etter GDPR artikkel 5 nr. 1 bokstav a skal personopplysninger «behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte».

At personopplysninger skal behandles på en «rettferdig» måte viser til **rettferdighetsprinsippet** og innebærer at registrertes interesser og rimelige forventninger må respekteres. EDPB underbygger denne tolkningen og påpeker i tillegg at

[96] NOU 2022: 11 s. 40.
[97] Se punkt 1.2.
[98] Datatilsynet, «Kunstig intelligens og personvern», rapport, 11. januar 2018, s. 15.

behandlingsansvarlige må vurdere og hensynta mulige virkninger av maktubalansen mellom registrerte og behandlingsansvarlige.[99]

De siste årene har KI-systemer ved flere tilfeller blitt diskriminerende. Et eksempel er Microsofts chatbot «Tay» som på under et døgn med chatting på Twitter i 2016 ble både høyreekstrem og kvinnefiendtlig.[100] At dette kan skje er en påminner om at maskinlæringsalgoritmene, enn så lenge, er et produkt av menneskene som skaper og interagerer med dem. Den resulterende diskrimineringen kan klassifiseres innenfor tre kategorier.[101] For det første kan det være forutinntatthet blant menneskene som lager algoritmen som anvendes i KI-systemet. For det andre kan det være forutinntatte holdninger i treningsdataen som brukes av algoritmen. For det tredje kan det være forutinntatte holdninger blant brukerne av systemet slik at det videreutvikles til å bli diskriminerende etter at det er ute på markedet.[102] Diskriminerende behandling av personopplysninger vil stride med rettferdighetsprinsippet og således være et brudd på GDPR.

I fortalen til GDPR er det foreslått å bruke egnede statistiske eller matematiske fremgangsmåter for å sikre at behandlingen blir rettferdig.[103] For å bestemme hva som er egnede matematiske eller statiske fremgangsmåter må det foretas risikovurderinger. Datatilsynet mener imidlertid at dette ikke er nok.[104] Modellene må i tillegg trenes på relevante og riktige opplysninger. Videre må de lære å ikke vektlegge opplysninger som kan medføre diskriminerende eller urettferdig behandling.[105]

At personopplysninger skal behandles på en «åpen måte» med «hensyn til den registrerte» jf. GDPR artikkel 5 nr. 1 bokstav a viser til **åpenhetsprinsippet.**

Ordlyden innebærer etter en alminnelig språkforståelse at behandlingen må være oversiktlig og forutsigbar. Behandlingen må videre være transparent gjennom hele prosessen. Åpenhets-

---

[99] EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, versjon 2, 8. oktober 2019, avsnitt 12.
[100] Eldrid Borgan, «Kunstig intelligens blir mannssjåvinistiske rasister. Hva kan vi gjøre for å stoppe det?», *Forskning.no*, 29. november 2019, [Tilgjengelig her: https://forskning.no/arbeid-it-juridiske-fag/kunstig-intelligens-blir-mannssjavinistiske-rasister-hva-kan-vi-gjore-for-a-stoppe-det/1599018] (lest 15.03.2023).
[101] Cofone (2019) s. 6.
[102] Ibid.
[103] GDPR fortalepunkt 71.
[104] Datatilsynet, «Kunstig intelligens og personvern», rapport, 11. januar 2018, s. 15.
[105] Ibid.

eller gjennomsiktighetsprinsippet er helt sentralt for å ivareta personers rett til å bestemme over opplysninger om seg selv.[106]

Utvikere av avanserte former for maskinlæringssystemer, slik som dyp læring, er ikke nødvendigvis selv klar over hvordan opplysninger brukes og vektlegges i systemet. I disse tilfellene er det tilnærmet umulig å gi tilstrekkelig informasjon til den registrerte.[107] Sett i lys av oppgavens problemstilling kan dette også medføre at det er utfordrende, og i noen tilfeller tilnærmet umulig, for utviklerne å foreta de risikovurderingene som kreves etter GDPR kapittel IV.[108]

3.3.2 Formålsbegrensning og dataminimering

Formålsbegrensningsprinsippet følger av GDPR artikkel 5 nr. 1 bokstav b. Prinsippet innebærer at innsamling av personopplysninger kun kan skje på bakgrunn av forhåndsdefinerte formål. Enhver behandling i etterkant av innsamlingen må være forenlig med det opprinnelige formålet. Dersom opplysninger behandles for andre formål enn det opprinnelige, trengs det et nytt behandlingsgrunnlag.[109]

Det er særlig to egenskaper ved KI-systemer som utfordrer formålsbehandlingsprinsippet. For det første kan det være vanskelig å definere et spesifikt og uttrykkelig angitt formål på forhånd. Det kan være utfordrende å forutse hva maskinlæringsalgoritmen lærer og følgelig hva den kan anvendes til. Dermed er det lett å havne i en situasjon med formålsutglidning. Det vil si at det definerte formålet glir ut og endrer seg i takt med det systemet lærer.

For det andre krever utvikling og bruk av KI mange ulike typer opplysninger. Det kan være fristende å sette et vidt mål, eksempelvis «forskning», for å kunne gjenbruke noen av disse.[110] Hvis de registrerte skal kunne ta et informert valg om hvilke opplysninger som behandles og hvorfor, kan ikke «forskning» godkjennes. Formålet må være mer konkretisert.

Risikovurderingene behandlingsansvarlig skal foreta må videre skje på bakgrunn av formålet med behandlingen.

---

[106] Datatilsynet, «Kunstig intelligens og personvern», rapport, 11. januar 2018, s. 18.
[107] Ibid.
[108] For gjennomgang av disse, se punkt 5.2.
[109] Datatilsynet, «Kunstig intelligens og personvern», rapport, 11. januar 2018, s. 17.
[110] Datatilsynet, «Kunstig intelligens og personvern», rapport, 11. januar 2018, s. 16.

Det må med andre ord vurderes om risikoen behandlingen utgjør for den registrerte er proporsjonal og legitim sett i lys av formålet med behandlingen.

At det kun er personopplysningene som er nødvendige for å oppnå det forhåndsdefinerte formålet som kan behandles fremgår også av **dataminimeringsprinsippet**. Etter dataminimeringsprinsippet skal personopplysningene være «adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for».[111] Ordlyden «begrenset til det som er nødvendig for formålet», medfører at dataminimeringsprinsippet er den enkleste måten å redusere risiko på. Når behandlingsansvarlig ikke trenger å behandle personopplysninger, skal hun ikke gjøre det.

Ordlyden «adekvate» og «relevante» viser videre til at det må samles inn tilstrekkelig med opplysninger for å nå målet med behandlingen, eksempelvis at KI-systemet blir funksjonelt. Samlet sett legges det opp til en proporsjonalitetsvurdering. Innsamlingen og behandlingen må ikke utgjøre et større inngrep overfor den registrerte enn hva som var nødvendig.[112]

I relasjon til KI kan det være vanskelig å ettergå hvilke opplysninger som var relevante for den beslutningen maskinlæringsalgoritmen kom til, og som dermed var nødvendige for å oppnå formålet. For å bøte på denne problematikken er det viktig at utviklerne løpende foretar nye vurderinger av hvilke personopplysninger som er nødvendig og sletter øvrige opplysninger. Det må videre vurderes om det finnes andre teknikker som legger til rette for at målet kan nås med mindre deling av data.

[111] GDPR art. 5 nr. 1 bokstav c.
[112] Datatilsynet, «Kunstig intelligens og personvern», rapport, 11. januar 2018, s. 17.

4. AI Act - Fremtidens regulering av kunstig intelligens

Som nevnt er formålet med AI Act er at KI skal kunne utvikle seg på en måte som både sikrer EUs grunnleggende friheter og rettighetene, garanterer tillit og sikkerhet, og samtidig fremmer innovasjon.[113]

Virkeområdet til AI Act fremgår av Rådets forslag artikkel 2 nr. 1. Bestemmelsen avgrenser virkeområdet mot produkter som ikke utvikles eller tilbys i EU. Det er først når produktet når EUs marked at AIA får anvendelse. Dette representerer en viktig forskjell fra GDPR sitt virkeområde. GDPR kommer som oftest også til anvendelse dersom personopplysninger om personer fra EU/EØS behandles utenfor EU/EØS.[114] Til illustrasjon medfører dette at leverandører som utvikler KI i en tredjestat, men hvor systemet er rettet mot EUs marked og behandler personopplysninger om innbyggere fra Unionen, må overholde GDPR fra starten. AIA kommer derimot først til anvendelse når produktet når EUs marked.[115]

For den videre fremstillingen er det hensiktsmessig å presentere forslaget til AI Act og systemet i dette. Dette gjøres i punkt 4.2. I punkt 4.1 forklares hvilke hovedaktører som har forpliktelser under AI Act og hvem disse er etter GDPR.

4.1 Hovedaktørene under AI Act

I Rådets forslag fortalepunkt 58a er det erkjent at leverandør og bruker kan ha rolle som behandlingsansvarlig eller databehandler etter GDPR. Utover dette mangler det beskrivelser av sammenhengen mellom disse pliktsubjektene og hvordan rollefordelingen vil utfolde seg i praksis. Dette medfører at det er behov for en konkret rolleavklaring. I det følgende skal leverandør og bruker under AI Act presenteres og det skal kartlegges hvilken rolle disse har under GDPR.

---

[113] Digdir, «Ny forordning for kunstig intelligens», u.å. [Tilgjengelig her: *Ny forordning for kunstig intelligens*] (sitert 01.04.2023).
[114] Etter GDPR art. 3 nr. 1 kommer GDPR til anvendelse «på behandling av personopplysninger som utføres i forbindelse med aktivitetene ved virksomheten til en behandlingsansvarlig eller en databehandler i Unionen, uavhengig av om behandlingen finner sted i Unionen eller ikke».
[115] Se imidlertid fotnote 192 der jeg stiller spørsmål ved om AIA i realiteten vil komme til anvendelse på et tidligere tidspunkt enn dette.

Et av de mest sentrale pliktsubjektene under AI Act er **leverandører** («providers») som utvikler et KI-system, setter dette på markedet eller som tar det i bruk under eget navn eller varemerke.[116] En leverandør kan tilby KI-systemet gratis eller mot betaling, og kan både være en fysisk eller juridisk person, offentlig myndighet, etat eller annet organ.[117] Imidlertid avgrenser Rådets forslag artikkel 2 nr. 4 mot myndigheter i tredjeland og internasjonale organisasjoner som bruker KI-systemer innenfor rammen av internasjonale avtaler. KI-systemet må isåfall brukes til rettshåndhevelse og rettslig samarbeid med ett eller flere av medlemslandene i Unionen.

Leverandøren er videre den aktøren som er ilagt flest forpliktelser etter AI Act. Forpliktelsene er mange og strekker seg fra alt fra teknisk dokumentasjon, journalføring og transparens til å måtte etablere sitt eget risikostyringssystem etter artikkel 9. Utover de forpliktelsene som direkte er ilagt leverandøren gjennom eksempelvis Rådets forslag artikkel 16, er det også de som først, før de kan tilby systemet til EUs marked, må vurdere hvilken risikokategori det faller inn under.

Også **bruker** («users») er en sentral aktør under AI Act. Brukere er definert i Rådets forslag artikkel 3 nr. 4 som «any natural or legal person, including a public authority, agency or other body, under whose authority the system is used». Dette kan eksempelvis være en arbeidsgiver som anvender et KI-system til å bistå med ansettelsesprosessen sin eller en bank som anvender KI til å identifisere risikolånetakere. Brukere er også illagt forpliktelser i AI Act, men i forhold til leverandørens er disse begrenset. Artikkel 29 pålegger brukere av høyrisikosystemer krav til å blant annet sørge for at dataen de tilfører systemet er relevant i lys av formålet. De skal også bruke informasjon mottatt av leverandøren til å gjennomføre en DPIA etter GDPR artikkel 35 dersom de er pålagt det.[118] Videre har brukere etter artikkel 52 en forpliktelse til å opptre transparent. Denne forpliktelsen innebærer blant annet å informere fysiske personer som er utsatte for visse KI-systemer.

Sett i lys av GDPR vil definisjonen av brukere i AIA i mange tilfeller være behandlingsansvarlige etter GDPR artikkel 4 nr. 7, mens leverandørene opptrer som databehandlere jf. GDPR artikkel 4 nr. 8, se punkt 3.3 og 5.2. Dette medfører at selv om brukernes forpliktelser etter AIA er begrenset, vil disse ha en rekke forpliktelser som

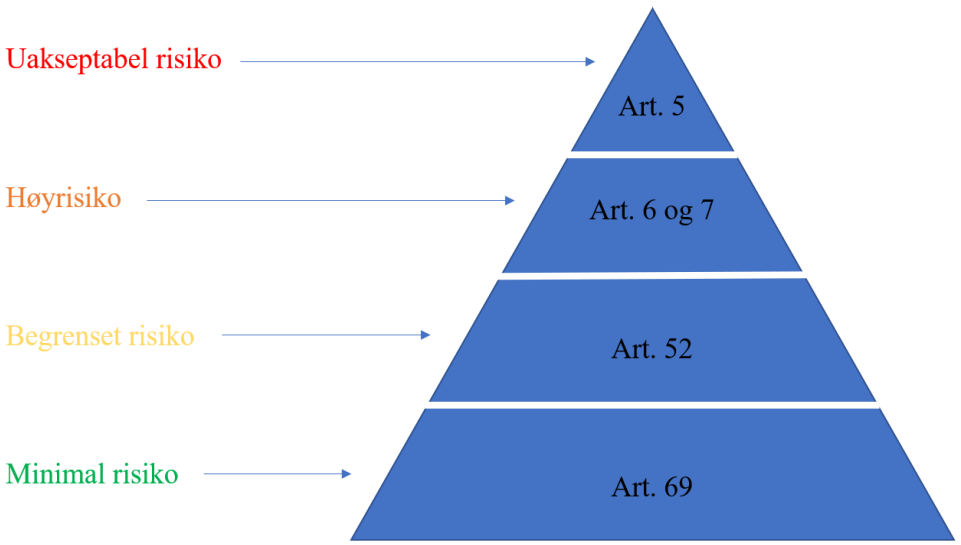
[116] Rådets forslag art. 3 nr. 2.
[117] Ibid.
[118] Rådets forslag art. 26 nr. 6. Se oppgavens punkt 5.3.

behandlingsansvarlige etter reglene i GDPR. Samtidig er leverandøren behandlingsansvarlig for behandling av personopplysninger som gjøres med det formål å utvikle, trene opp og videreutvikle KI-systemet sitt. Leverandører opptrer derfor i mange tilfeller som databehandler og behandlinganSvarlig samtidig. Rollefordelingen i GDPR og AI Act samlet sett forklares nærmere i punkt 5.3.1. Poenget er likevel at ansvaret for risiko og hvem som må foreta risikovurderinger vil være ulikt i de to regelverkene og at det kan være utfordrende å identifisere hvilke rolle man har.[119]

Det er også oppstilt forpliktelser for andre aktører, inkludert **distributører**[120] og **importører**[121] med hensikt å stoppe farlige produkter utviklet utenfor EU fra å komme inn i EUs marked jf. Rådets forslag artikkel 26 og 27. Oppgaven avgrenser imidlertid mot andre aktører enn leverandører og brukere, se punkt. 1.4.1.

4.2 Forslaget til AI Act - en risikobasert tilnærming til KI

AIA oppstiller fire risikogrupper; *minimal risiko, begrenset risiko, høy risiko og uakseptabel risiko*. Systemet innebærer at jo høyere risiko bruk av en KI utgjør, jo større trussel utgjør den mot samfunnet og jo strengere må den reguleres.[122] Dette medfører videre at de fleste reguleringer i AIA retter seg mot systemer som utgjør en høy risiko.



[119] Mer om dette i punkt 5.3.
[120] Definert i Rådets forslag art. 3 nr. 7 som «any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market».
[121] Definert i Rådets forslag art. 3 nr. 6 som «any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market».
[122] Kommunal- og distriktsdepartementet, «Forslag til forordning om kunstig intelligens (KI-forordningen)», EØS-notat, 21. juni 2021, sist oppdatert 12. november 2021.

Figur 2: Risikogruppene i AIA

4.2.1 Uakseptabel risiko - Forbudt

Artikkel 5 i Rådets forslag regulerer KI-systemer som er forbudt å tilby eller bruke. Dette er systemer som medfører brudd på grunnleggende rettigheter og friheter i EU.[123] Kommisjonen og Rådet har vært stort sett enige om denne opplistingen, mens Parlamentet har foreslått å utvide listen.[124]

Ulovlige KI-systemet omfatter foreløpig subliminale teknikker, manipulasjon, «social scoring»-systemer slik som har blitt brukt i nyere tid i Kina og sanntids biometriske identifikasjonssystemer, men med unntak.[125]

4.2.2 Høyrisko

Høyrisiko KI-systemer er underlagt et detaljert sertifiseringsregime, men anses ikke så grunnleggende kritikkverdige at de burde bli forbudt. Høyrisikosystemer er systemer som kan medføre en betydelig risiko for helse, sikkerhet eller EUs grunnleggende rettigheter.[126]

Dette er for det første KI-systemer som i seg selv reguleres av harmonisert EU-lovgivning oppført i vedlegg II til Rådets forslag. De må imidlertid være «required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product» etter denne lovgivningen.[127] Vedlegg II-A lister opp EU-rettsakter som regulerer KI-systemer anvendt som sikkerhetskomponenter i produkter, eksempelvis maskiner eller medisinsk utstyr. Vedlegg II-B lister opp andre harmoniserte EU-rettsakter, herunder EU lovgivning som omhandler båter, jernbane, motorer, kjøretøyer og så videre.[128]

For det andre skal systemer opplistet i vedlegg III til Rådets forslag som hovedregel automatisk betraktes som høyrisiko.[129] Som nevnt i punkt 1.4.2 foreslår Parliamentet at de ikke automatisk skal være høyrisiko, men at det må foretas en vurdering av om de medfører en betydelig risiko for helse, sikkerhet eller EUs grunnleggende rettigheter.

---

[123] Ibid.
[124] Se punkt 1.4.1.
[125] Ordlyden er oversatt til norsk av Kommunal- og distriktsdepartementet i «Forslag til forordning om kunstig intelligens (KI-forordningen)», EØS-notat, 21. juni 2021, sist oppdatert 12. november 2021.
[126] Rådets forslag art. 6 nr. 3 og art. 7 nr. 1 bokstav b.
[127] Rådets forslag art 6 nr. 1 og nr. 2.
[128] Edwards (2022) s. 14.
[129] Rådets forslag art 6 nr. 3.

Vedlegg III inneholder per 30. april 2023 en liste med åtte høyrisiko KI-systemer. Disse er blant annet KI-systemer som brukes i drift og styring av kritisk infrastruktur, slik som buss og tog. Videre er det systemer som brukes til utdannings- og yrkesopplæringsformål, inkludert systemer som bestemmer hvem som får tilgang til utdanning eller yrkesopplæring. Deretter er det KI-systemer brukt i ansettelsesprosesser eller av en arbeidsgiver overfor sine ansatte. Eksempelvis automatiserte ansettelsesprosesser eller CV-gjennomganger.[130] Listen inneholder også viktige offentlige systemer, herunder systemer som gir tilgang til offentlige tjenester og systemer for håndtering av migrasjon, asyl og grensekontroll.

Denne listen består både av systemer som finnes i dag og systemer som er i ferd med å utvikles. Listen skal kunne utvides og det skal etableres en database over høyrisikosystemer administrert av Kommisjonen.[131]

Bruk av høyrisikosystemer skal være lovlig såfremt de er i tråd med reglene i AIA Del III kapittel 2. Reglene innebærer blant annet at KI-systemene må være underlagt et risikostyringssystem, det må gis detaljert informasjon om hvordan de fungerer og det må foreligge menneskelig tilsyn.[132]

Rådet har gjort flere endringer fra Kommisjonens originale forslag i kravene til høyrisikosystemer. Blant annet, og av relevans for denne oppgaven, er det forsøkt å tydeliggjøre ansvarsfordelingen og rollene til de ulike aktørene, særlig leverandører og brukere av KI-systemer. Rådets forslag klargjør også flere steder forholdet mellom ansvar i henhold til AIA og ansvar som allerede eksisterer under annen lovgivning, herunder GDPR.[133] Videre har Parlamentet foreslått å utvide listen, se punkt 1.4.1.

4.2.3 Begrenset risiko

Fire KI-systemer med begrenset risiko er definert i AI Act artikkel 52. Innholdet i Kommisjonens forslag og Rådets forslag samsvarer, men det er gjort noen endringer i ordlyden. I Rådets forslag er alle de fire systemene definert under egne punkter.

[130] Eksempler henter fra Edwards (2022) s. 14.
[131] Kommunal- og distriktsdepartementet, «Forslag til forordning om kunstig intelligens (KI-forordningen)», EØS-notat, 21. juni 2021, sist oppdatert 12. november 2021.
[132] Ibid.
[133] Council of the EU, «Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights», pressemelding, 6. desember 2022.

KI-systemer med begrenset risiko er lovlige å bruke, men leverandørene og brukerne er underlagt visse forpliktelser til å være transparente.

De fire systemene er for det første systemer som har som formål å interagere/samhandle med mennesker, eksempelvis «chatbots». For det andre er det biometriske kategoriseringssystemer. For det tredje er det KI-systemer for å gjenkjenne emosjoner («emotion recognition systems»). Til sist utgjør også «deep fakes» som hovedregel begrenset risiko. Deep fakes er manipulerte videoer eller bilder der ansiktet og/eller stemmen til en person erstattes med en annen persons ansikt og/eller stemme.[134]

Transparenskravet går ut på at mennesker som hovedregel må informeres om at de samhandler med et av de ovennevnte KI-systemene dersom det ikke fremgår åpenbart ut fra sammenhengen. Denne plikten er pålagt leverandørene av systemer som interagerer med mennesker (chatbots), mens den ligger på brukere av de andre tre systemene.

Forpliktelsene etter artikkel 52 vil i stor grad overlappe med kravene til transparens etter GDPR og åpenhetsprinsippet etter GDPR artikkel 5 nr. 1 bokstav a. Etter GDPR artikkel 13 nr. 2 bokstav f og 14 nr. 2 bokstav g skal det gis opplysningen om «forekomsten av automatiserte avgjørelser, herunder profilering, som nevnt i artikkel 22 nr. 1 og 4, og, i det minste i nevnte tilfeller, relevant informasjon om den underliggende logikken samt om betydningen og de forventede konsekvensene av en slik behandling for den registrerte». Disse forpliktelsene pålegges behandlingsansvarlige. I praksis medfører det at selv om leverandøren er den som skal gi informasjon etter AIA ved bruk av KI-systemer som samhandler med mennesker (chatbots), må trolig brukeren gi denne informasjonen etter GDPR, så lenge det er brukeren som opptrer som behandlingsansvarlig. Det foreligger per nå ingen avklaringer av hvordan denne potensielle overlappen vil utspille seg i praksis.

4.2.4 Minimal risiko

De fleste av dagens KI-systemer utgjør minimal risiko.[135] Dette er alle systemer som ikke defineres under de tre andre risikogruppene, eksempelvis spam-filtre. For denne gruppen oppstiller ikke AIA noen særskilte forpliktelser, men Kommisjonens foreslår at disse systemene bør reguleres i frivillige Codes of Conduct.[136] Reguleringer i Codes of Conducts behandles i artikkel 69.

[134] Rådets forslag art. 52 nr. 3.
[135] Ibid.
[136] Exploratory memorandum til Kommisjonens forslag punkt 5.2.7.

5. Risikovurderinger etter AI Act i lys av risikovurderinger etter GDPR

I dette kapittelet skal de risikobaserte tilnærmingene presentert i punkt 1.2 først oppsummeres kort. Derettes skal det utgreies hvilke konsekvenser det får at den overordnede risikobaserte tilnærmingen i AI Act skiller seg betraktelig fra GDPR. Dette gjøres i punkt 5.1.

Videre er det flere bestemmelser som oppstiller konkrete krav til gjennomføring av risikovurderinger i GDPR og AI Act. For å kunne besvare problemstillingen om hvordan risikovurderingene i GDPR og AI Act samspiller må også disse kravene analyseres og sammenlignes. Dette skal gjøres i punkt 5.2 og 5.3. I GDPR finner vi disse bestemmelsene i kapittel IV og i AI Act finner vi de i Rådets forslag artikkel 9 samt i bestemmelsene som upensler de ulike risikokategoriene.[137]

5.1 Hva er konsekvensene av at de risikobaserte tilnærmingene i AI Act og GDPR er ulike?

Både AI Act og GDPR har en risikobasert tilnærming, se punkt 1.2. I GDPR er denne nedfelt i blant annet ansvarlighetsprinsippet i artikkel 5 nr. 2 samt artikkel 24 og 32. Formen for risikostyring i GDPR følger et *nedenfra-og-opp*-perspektiv.[138] Med dette menes at evalueringen av risiko og valg av risikoreduserende tiltak ikke er definert av loven, men overlatt til behandlingsansvarliges skjønn.[139] AIA representerer det motsatte synspunktet. Selve risikokategoriseringen overlates ikke til aktørene som forordningen retter seg mot.[140] Det er AIA som selv, fra en *ovenfra-og-ned*-tilnærming, identifiserer direkte de ulike risikokategoriene gjennomgått i punkt 4.2.

Ulikhetene i de risikobaserte tilnærmingene kan føre til at det blir utfordrende å få en helhetlig forståelse av risiko og hvilket ansvar risikoen medfører. Selv om det må vurderes hvilken risikokategori et KI-system ligger innunder, ansvarliggjøres leverandørene i mindre grad for denne vurderingen enn hva behandlingsansvarlig gjør etter GDPR når rommet for skjønn er større. I ytterste konsekvens, kan det medføre en fragmentering av EUs lovgivning.

[137] Rådets forslag art. 5, 6,7, 52 og 69.
[138] De Gregorio og Dunn (2022) s. 4.
[139] Se punkt 1.2.
[140] De Gregorio og Dunn (2022) s. 4.

Ikke bare for reguleringen av det indre marked, men også på konstitusjonelt nivå.[141] På den andre siden er det det samme konstitusjonelle målet om å fremme EUs grunnleggende rettigheter og friheter, herunder personvern, som er bakgrunnen for de to regelverkene, se punkt 1.3. De deler et ønske om å regulere, og dermed minimere, risikoen nye teknologier utgjør. Selv om de gir uttrykk for EUs risikobaserte tilnærming på svært ulike måter, er dette overordnede målet en samlende faktor.[142] Når GDPR ikke alene har klart å begrense risikoene KI utgjør for menneskers rettigheter og friheter på en tilstrekkelig måte, er det kanskje nødvendig at AI Act har en så ulik tilnærming til risiko. Det vil være lettere å identifisere om en aktør har feilkategorisert et KI-system etter AI Act enn å ettergå risikovurderingene foretatt etter GDPR. Samtidig favner GDPR mye videre og omhandler situasjoner som kun kan reguleres samlet med et teknologinøytralt regelverk.

5.2 Hvilke krav pålegges behandlingsansvarlige og databehandlere etter GDPR?

Som nevnt må de konkrete risikovurderingene lovfestet i GDPR artikkel IV og i AI Act utgreies. Dette må gjøres for at det i punkt 5.3 skal kunne vurderes hva overholdelse av disse innebærer for hovedaktørene i praksis, og hva de må være bevvist for å unngå negative konsekvenser.

Bestemmelsene som skal vurderes i dette kapittelet er GDPR artikkel 24, 25, 32 og 35. Oppgaven tar for seg disse bestemmelsene fordi de på ulike måter pålegger behandlingsansvarlig eller databehandler å arbeide risikobasert. Det er andre bestemmelser som også fasiliterer risikovurderinger, herunder artikkel 34. Disse gjelder imidlertid etter at et brudd på personvernsikkerheten er stadfestet eller utpensler de videre konsekvensene av risikovurderingene, og skal ikke behandles.

Felles for alle bestemmelsene er at det er risikoen for «fysiske personers rettigheter og friheter» som skal vurderes.[143] Dette skiller seg fra AI Act der risikoen for samfunnet og for EUs grunnleggende rettigheter og friheter mer overordnet er temaet, se punkt 4.2. Bestemmelsene som skal behandles skiller seg fra hverandre ved at de legger opp til ulike tiltak på bagrunn av ulike vurderinger. Artikkel 24 legger opp til en bred og generell

[141] Ibid.
[142] Ibid.
[143] Schartum (2020) s. 239.

vurdering av tiltak for å sikre og påvise etterlevelse av forordningen. Artikkel 25 utpensler og pålegger krav om innebygde tiltak og artikkel 32 omhandler behandlingens sikkerhet.[144] Til sist inneholder 35 krav om å vurdere konsekvensene av risikoen og håndtere disse.

5.2.1 GDPR artikkel 24

Ved siden av ansvarlighetsprinsippet, underbygger også artikkel 24 at GDPR er en risikobasert rettsakt. Temaet i bestemmelsen er risikoen for manglende etterlevelse av forordningen.[145] Med dette menes at den, ved å forutsette en bred og generell vurdering av tiltak, både skal sikre etterlevelse og at ellerlevelsen skal kunne påvises.[146]

Det følger av GDPR artikkel 24 nr. 1 at:

> *Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige gjennomføre* ***egnede tekniske og organisatoriske tiltak*** *for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.*[147]

Det er følgelig artikkel 24 som utpensler de konkrete hensynene og tiltakene som må iverksettes og dokumenteres for å kunne overholde ansvarlighetsprinsippet etter artikkel 5 nr. 2. At tiltakene skal «gjennomgås på nytt» og «oppdateres ved behov» viser til at denne internkontrollen er en løpende aktivitet.[148] I praksis innebærer dette at behandlingsansvarlig løpende må foreta risikovurderinger for å sikre og påvise etterlevelse av GDPR.

I fortalepunkt 75 er det listet opp ulike risikosituasjoner den behandlingsansvarlige må være bevisst på i risikovurderingen og i fortalepunkt 76 gis det veiledning til hvordan risikovurderingen kan foretas. Etter fortalepunkt 74 må de egnede tekniske og organisatoriske tiltakene videre være effektive, dermed må behandlingsansvarlig foreta en proporsjonalitetsvurdering og iverksette de tiltakene som er proporsjonale i henhold til risikoen for den registrerte.

---

[144] Ibid.
[145] Schartum (2020) s. 239.
[146] Ibid.
[147] Min uthevning.
[148] Eva Jarbekk, «Karnov lovkommentar til personvernforordningen.», *i Lovdata Pro* (2021) artikkel 24 note 2.

5.2.2 GDPR artikkel 25

Artikkel 25 nr. 1 inneholder for det første en plikt til å bygge inn personvern («privacy by design») og vilkårene for at denne plikten skal foreligge.[149] Det fremgår deretter at denne plikten foreligger «både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve behandlingen». At plikten foreligger allerede på tidspunktet for fastsettelsen av midlene medfører at bestemmelsen får betydning for utvikling av nye tjenester og produkter.[150] Dette fører videre til at behandlingsansvarlig har en handlingsplikt etter artikkel 25 nr. 1 når det skal vurderes om et KI-system som behandler personopplysninger kan anvendes i deres tjeneste.

EDPB poengterer videre i sin veiledning om artikkel 25 at det at plikten foreligger på tidspunkt for selve behandlingen, medfører at den også gjelder for behandling foretatt av databehandlere.[151] Det er imidlertid fortsatt behandlingsansvarlig som er ansvarlig for risikoen, men databehandlers operasjoner må jevnlig gjennomgås og vurderes for å sikre kontinuerlig overholdelse av bestemmelsen.[152]

Artikkel 25 nr. 2 utpensler reglene for personvern som standardinnstilling. Ordlyden er bygd opp på samme måte som artikkel 25 nr. 1, men i motsetning til de vage og vide kravene etter første punkt, inneholder 25 andre punkt relativt spesifikke krav.[153] Som standard skal behandling av personopplysninger maksimalt omfatte mengden personopplysninger som er nødvendig for å oppfylle formålet med behandlingen, det omfanget av behandling formålet kan begrunne og varigheten og tilgjengeligheten som formålet tillater.[154] I tillegg skal personopplysninger som standard «ikke gjøres tilgjengelige for et ubegrenset antall fysiske personer uten den berørte personens medvirkning».[155]

Artikkel 25 nr. 2 er en presisering av dataminimeringsprinsippet etter GDPR artikkel 5 nr. 1 bokstav c.[156] Bestemmelsen gir i utgangspunktet ikke uttrykk for noe mer eller annet enn det som fremgår av dette.[157] En slik forståelse er også lagt til grunn av EDPB som poengterer at

[149] Schartum (2020) s. 249.
[150] Jarbekk (2021) artikkel 25 note 2.
[151] EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, vedtatt 13. november 2019, avsnitt 39.
[152] Ibid.
[153] Schartum (2020) s. 261.
[154] Ibid.
[155] GDPR art. 25 nr. 2 siste setning.
[156] Se punkt 3.3.2 forgjennomgang av dataminimeringsprinsippet.
[157] Schartum (2020) s. 261.

artikkel 25 nr. 2 lister opp de dimensjonene av dataminimeringsprinsippet som skal være standard.[158]

I likhet med både artikkel 24 og 32 er et av hovedfokusene i artikkel 25 «risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter». Denne skal begrenses ved å iverksette «egnede tekniske og organisatoriske tiltak». Med andre ord oppstilles det krav til aktiv handling for å begrense risikoen for den registrerte. Dette er en direkte risikobasert tilnærming der behandlingsansvarlig er pålagt å foreta risikovurderinger utover det overordnede ansvaret for risikostyring som følger av artikkel 5 nr. 2.[159]

5.2.3 GDPR artikkel 32

En bestemmelse som også kan brukes til å begrunne at GDPR er en risikobasert rettsakt er artikkel 32. Temaet i artikkel 32 er personopplysningssikkerhet. Brudd på personopplysningssikkerheten er definert i GDPR artikkel 4 nr. 12 som et «brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.». Ordlyden kan forstås som en positiv angivelse av hva personopplysningssikkerhet er.[160]

Personopplysningssikkerhet er videre behandlet i GDPR artikkel 5 nr. 1 bokstav f som oppstiller konfidensialitet- og integritetsprinsippet. Etter artikkel 5 nr. 1 bokstav f skal personopplysninger «behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak.».

Artikkel 32 må dermed sees i lys av disse bestemmelsene. En viktig forskjell fra konfidensialitet- og integritetsprinsippet og fra både artikkel 24 og 25 er at ansvaret etter artikkel 32 pålegges både behandlingsansvarlig og databehandler. Dermed er begge disse hovedaktørene ansvarlige for risikovurderingene som må foretas etter bestemmelsen. Dette er interessant sett i lys av AI Act. Der plikten ikke samsvarer med en plikt brukeren har etter AI Act, må den som opptrer som bruker i relasjon til AI Act og databehandler i relasjon til GDPR være bevisst på at det må gjøres selvstendige analyser etter de to regelverkene. Dette kommer jeg tilbake til under punkt 5.3.

[158] EDPB, retningslinje 4/2019, avsnitt 48.
[159] Jarbekk (2021) artikkel 25 note 2.
[160] Schartum (2020) s. 262.

Helt konkret gir artikkel 32 nr. 1 en liste over tekniske og organisatoriske tiltak som databehandler eller behandlingsansvarlig kan gjennomføre for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Listen er ikke uttømmende. For å vurdere hvilke av disse eller andre tiltak som er nødvendige og egnet og som derfor skal iverksettes, må det foretas en risikovurdering av hver behandling.[161] I denne må det vurderes hvilken risiko behandlingen utgjør for den registrerte, formål med behandlingen og kostnadene ved den.[162] Fortalepunkt 78 lister opp flere tekniske og organisatoriske tiltak som kan iverksettes, herunder innebygd personvern og personvern som standardinnstilling jf. GDPR artikkel 25. I realiteten medfører dette at også databehandler kan måtte foreta risikovurderinger av samme behandling som behandlingsansvarlig for å overholde forpliktelsen sin etter artikkel 32 nr. 1.

GDPR artikkel 32 nr. 2 lister videre opp vurderingstemaer som skal vektlegges i risikovurderingen. Heller ikke denne opplistingen er uttømmende. I likhet med for artikkel 24 kan det sees hen til fortalepunkt 75 for flere ulike risikosituasjoner en må være bevisst på i risikovurderingen. Også dette tilsier at databehandler kan komme til å måtte gjøre mange lignende risikovurderinger som behandlingsansvarlig. Konsekvensen er, som nevnt, at databehandler må gjennomføre flere lignende vurderinger etter GDPR og AI Act uten at det er avklart i AI Act hvordan dette kan gjøres eller sammenstilles uten å skape store merkostnader.

5.2.4 GDPR artikkel 35

Etter artikkel 35 nr. 1 skal den behandlingsansvarlige foreta en vurdering av personvernkonsekvenser dersom det er sannsynlig at behandlingen medfører en «høy risiko» for fysiske personers grunnleggende rettigheter og friheter. Dette gjelder særlig «ved bruk av ny teknologi».

Ordlyden viser til at det skal foretas en personvernkonsekvensvurdering/Data Protection Impact Assessment (DPIA). Artikkel 35 inneholder videre regler for når en DPIA skal foretas, hva den minst skal inneholde og hvordan den skal utføres. Bestemmelsen er lang, og det kan isolert sett være vanskelig for en bedrift å forstå hva disse reglene innebærer for dem. Imidlertid har en rekke aktører publisert inngående veiledninger for hvordan DPIAer skal utføres i praksis. Allerede i 2017 publiserte A29-gruppen sin veiledning.[163] Her i Norge har Datatilsynet lagd en egen norsk veiledning basert på denne.[164]

[161] Jarbekk (2021) artikkel 32 note 2.
[162] Ibid.
[163] A29-gruppen, DPIA-retningslinje.
[164] Datatilsynet, «Vurdering av personvernkonsekvenser (DPIA)», veileder, sist endret 17. juli 2019.

Kravet om å foreta en DPIA foreligger dersom det er «sannsynlig» at behandlingen «vil medføre en høy risiko for fysiske personers rettigheter og friheter».[165] Ordlyden legger opp til en konkret skjønnsmessig vurdering. Samtidig oppstiller GDPR flere utgangspunkter for denne.[166] Som gjennomgått i punktene ovenfor skal det foretas risikovurderinger etter artikkel 24, 25 og 32. Både vurderingen av om det er «sannsynlig» at behandlingen medfører høy risiko etter 35 nr. 1 og risikovurderingene etter 24,25 og 32 skal foretas før behandling. Dermed begrunner nok ikke artikkel 35 nr. 1 en ny og separat risikovurdering. Basert på risikovurderingne som må foretas av artikkel 24, 25, 32 og 35 nr. 1 samlet sett, vil man kunne bestemme om risikoen er høy og dermed om det må iversettes en DPIA etter de øvrige reglene i artikkel 35.[167]

Et viktig poeng ved bruk av KI er at ordlyden i artikkel 35 nr. 1 «særlig ved bruk av ny teknologi» tilsier at det i praksis alltid må foretas en DPIA ved bruk av kunstig intelligens. Det samme gjelder ordlyden i artikkel 35 nr. 3 bokstav a om at en DPIA «særlig [vil] være nødvendig» ved en «systematisk og omfattende vurdering av personlige aspekter ved fysiske personer som er basert på automatisert behandling, herunder profilering, og som danner grunnlag for avgjørelser som har rettsvirkning for den fysiske personen eller på lignende måte i betydelig grad påvirker den fysiske personen». Sistnevnte viser til automatisert behandling regulert i artikkel 22 og medfører at det i alle tilfeller må foretas en DPIA ved slik bruk. Datatilsynet har også fastslått at det som oftest skal foretas en DPIA når personopplysninger behandles med innovativ teknologi slik som kunnstig intelligens.[168]

I artikkel 35 nr. 7 oppstilles minimumskravene til DPIAen, det vil si hva som i alle tilfeller må med i denne risikovurderingen. Dette er:

a) *En systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen.*
b) *En vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene.*
c) *En vurdering av risikoene for de registrertes rettigheter og friheter (...)*

[165] GDPR art. 35.
[166] Schartum (2020) s. 276.
[167] Ibid.
[168] Datatilsynet, veileder om DPIA, kapittel 2. I denne veilederen har Datatilsynet publisert en liste over behandlingsaktiviteter som alltid krever at det gjennomføres en DPIA. Denne listen er godkjent av EDPB. Flere av de opplistede behandlingsaktivitetene vil regnes som høyrisiko etter AIA.

d) *De planlagte tiltakene for å håndtere risikoene (...) og for å påvise at forordningen overholdes. (...)*

Deretter må behandlingsansvarlig evaluere resultatene og eventuelt godkjenne behandlingen.[169] Det er styret som har den viktigste rollen her og når konsekvensvurderingen er sammenstilt, skal funnene presenteres for ledelsen.[170]

Fra et risikostyringsperspektiv er formålet med en DPIA å håndtere risikoen. Dette gjøres ved å fastslå sammenheng, vurdere risikoene og til slutt håndtere den.[171]

5.3 Hvilke krav pålegges leverandører og brukere etter AI Act sammenlignet med forpliktelsene etter GDPR?

I den videre analysen skal hvilke risikovurderinger som må foretas etter GDPR og AI Act sammenstilles. Deretter skal det forklares hvem som skal foretas disse, når og hvordan de samspiller med hverandre.

Risikovurderingene som må foretas er inndelt i tid. Inndelingen i tid gir utgangspunktet for å kunne lage en figur i punkt 5.3.3 som illustrerer alle risikovurderingene som må foretas i løpet av livsløpet til en KI.

5.3.1 Risikovurderinger før utvikling til ferdig KI-system

Som gjennomgått under punkt 5.2 må behandlingsansvarlig etter GDPR artikkel 24, 25, 32 og 35 nr. 1 foreta risikovurderinger før et KI-system tas i bruk. Disse risikovurderingene gir blant annet svaret på om det er sannsynlig at systemet utgjør en høy risiko, slik at plikten til å foreta en DPIA etter GDPR artikkel 35 foreligger.

Etter AI Act foreligger en plikt til å vurdere risiko når KI-systemet skal tas i bruk i EU.[172] For å identifisere hvilke forpliktelser en leverandør har etter AI Act må vedkommende foreta en vurdering av hvilken kategori systemet som utvikles faller inn under, se oppgaven punkt 4.2. I denne vurderingen må leverandøren blant annet vurdere reglene i AI Act artiklene 5, 6,7, 52, 69. I motsetning til å betro leverandørene og brukere av KI-systemer oppgaven med å utvikle sitt eget risikoreduserende system, slik tilfellet er for behandlingsansvarlige og databehandler

[169] Datatilsynet, veileder om DPIA, kapittel 5.
[170] Ibid.
[171] Ibid.
[172] Rådets forslag art. 2 nr. 1, se punkt 4.

etter reglene i GDPR, begrenser AIA rommet for skjønn.[173] Med dette menes at når det er strengt regulert hvilke risikokategori et KI-system faller inn under, begrenses leverandørens spillerom betydelig ved utførelse av risikovurderingen.[174] Hovedskillet mellom GDPR og AIA går derfor ved hvordan man utfører slike risikovurderinger og hvem som er ansvarlig for gjennomføringen.[175]

Etter GDPR artikkel 5 nr. 1 er det behandlingsansvarlig som har denne oppgaven og som er ansvarlig for risikoen.[176] Derimot er det ingen av reglene i noen av versjonene av forslaget til AI Act som spesifiserer helt konkret hvem som er overordnet ansvarlig for risikoen. Pliktsubjektene er personlig ansvarlig for de forpliktelser som følger av forordningen og for de risikovurderingene som må foretas i tråd med disse. Imidlertid er det leverandøren som før et KI-systemet tilbys i Unionen, må vurdere hvilken risikokategori dette ligger innunder. Dette medfører at det i realiteten er leverandøren som er hovedansvarlig for risikoen og som risikerer å sanksjoneres etter AIA Del X dersom de har kategorisert systemet feil og følgelig ikke overholder forpliktelsene sine etter del III kapittel 2.[177] Samtidig må det understrekes at dersom leverandøren har feilkategorisert systemet, vil dette også kunne føre til at brukere ikke overholder sine forpliktelser og følgelig sanksjoneres for det. Derfor må trolig brukerne også utføre egne risikovurderinger før de tar systemet i bruk.

Videre er ikke vurderingen som må foretas av leverandøren for å kategorisere systemet sitt etter AI Act, lik risikovurderingene som må foretas etter GDPR. Listen over forbudte KI-systemer er direkte fastsatt av AI Act artikkel 5 og er uavhengig av eventuelle selvstendige risikovurderinger fra leverandører eller brukere av disse systemene.[178] Vurderingen av om et system er høyrisiko under AI Act er også en ren gjennomgang av om systemet faller inn under noen av de opplistede kategoriene i forordningens vedlegg III jf. Rådets forslag artikkel 6 nr. 2. Eventuelt om det er et produkt omfattet av de harmoniserte EU-rettsakterne opplistet i vedlegg II til forordningen og det etter disse er krav om å foreta en «third-party conformity assessment [...]» jf. Rådets forslag artikkel 6 nr. 1.[179]

[173] De Gregorio og Dunn (2022) s. 14.
[174] Ibid.
[175] De Gregorio og Dunn (2022) s. 14.
[176] Ibid.
[177] Rådets forslag art. 16 bokstav a.
[178] De Gregorio og Dunn (2022) s. 16.
[179] Se oppgavens punkt 4.2.2.

Derimot er det Kommisjonen som etter artikkel 7 må foreta en risikovurdering som i noen grad vil overlappe med vurderingene som må foretas av behandlingsansvarlig etter GDPR. Kommisjonen kan nemlig tilføye systemer som kan medføre en betydelig risiko for helse, sikkerhet eller grunnleggende rettigheter til listen over høyrisikosystemer i vedlegg III jf. Rådets forslag artikkel 7 nr. 1 bokstav b. Som gjennomgått i punkt 1.3 er personvern en av EUs grunnleggende rettigheter. Rådets forslag artikkel 7 setter også en rekke andre risikokriterier, men disse er alle ment som en veiledning for Kommisjonen selv, og ikke for de øvrige pliktsubjektene.[180]

Videre vil rollene til aktørene være ulike for ulike deler av behandlingen av personopplysninger slik at kompleksiteten ved overholdelse øker ytterligere. Dersom et system utvikles etter initiativ fra leverandøren selv og utviklingen ikke er bestilt av en bruker, er det som oftest leverandøren som er behandlingsansvarlig i relasjon til GDPR i utviklingsfasen, og løpende til videreutvikling av systemet. Dette er tilfellet så lenge systemet behandler personopplysninger, eksempelvis som treningsdata, og denne behandlingen faller inn under GDPR sitt saklige og geografiske virkeområde etter GDPR artiklene 2 og 3. I disse tilfellene må leverandøren foreta risikovurderingene pålagt etter GDPR artikkel 24, 25, 32 og 35 før utviklingen og følgelig før behandlingen starter.[181] Når systemet er klart til å tilbys EUs marked, må det foretas en ny risikovurdering av leverandøren for å vurdere hvilken risikokategori systemet faller inn under etter AI Act. Dette gjøres ved å vurdere reglene i artikkel 5, 6,7, 52 og 69 gjennomgått i punkt 4.2. Etter at en bruker etablert i EU har tatt systemet i bruk er det derimot brukeren som er behandlingsansvarlig for de delene av behandlingen leverandøren gjør på vegne av brukeren.

Samlet sett må hovedaktørene foreta ulike vurderinger på ulike tidspunkter. Videre er det ulike aktører som er ansvarlig for risikoen under regelverkene og rollefordelingen vil være ulik for ulike deler av behandlingen.

Ansvaret og rollefordelingen kan illustreres ved å se på et eksempel. Et norsk oppstartsselskap utvikler et KI-system som kan bistå med CV-gjennomganger for bedrifter i EU/EØS i deres ansettelsesprosesser. Dette er en idé oppstartsbedriften har fått på egenhånd og når de starter å utvikle systemet innhentes det mange CV-er for å trene det opp. Disse inneholder en rekke personopplysninger. Når produktet er klart til å tilbys markedet, er det mange selskaper som

[180] De Gregorio og Dunn (2022) s. 16.
[181] Se gjennomgang av disse under punkt 5.2.

ønsker å benytte seg av det. Et av dem er et tysk selskap. De har som formål å effektivisere sine ansettelsesprosesser og synes KI-systemet er et fint teknisk virkemiddel til å nå dette målet.

I dette eksempelet vil oppstartselskapet først selv være behandlingsansvarlig jf. GDPR artikkel 4 nr. 7. Det er de som har som formål å trene opp systemet sitt og følgelig må foreta risikovurderinger etter GDPR artikkel 24, 25, 32 og 35 før behandlingen av CVene. Når systemet er ferdig og de leverer dette til det europeiske markedet vil de være leverandør i relasjon til AI Act artikkel 3 nr. 2 og må kategorisere systemet innenfor AIA sine risikokategorier.[182] Mens de behandler personopplysninger på vegne av en av brukerne av systemet, vil de være databehandlere i relasjon til GDPR artikkel 4 nr. 8 og må foreta vurderinger etter GDPR artikkel 32. Samtidig er det tyske selskapet behandlingsansvarlig og må foreta egne risikovurderinger etter artikkel 24, 25, 32 og 35 og eventuelt gjennomføre en DPIA etter GDPR art. 35 før de tar systemet i bruk.[183] Det tyske selskapet er også brukere etter AI Act og må overholde sine forpliktelser etter blant annet Rådets forslag artikkel 29. Overfor personopplysninger oppstartselskapet bruker til å videreutvikle sitt eget system fortsetter de å være behandlingsansvarlige.

Det er liten tvil om at det kan være utfordrende å overholde begge regelverkene fullt ut når rollene og ansvarsområdene for risikoen endrer seg på denne måten. Samtidig er GDPR bygget opp slik at risikovurderingene neppe kan samordnes. Som gjennomgått under punkt 5.2 er risikovurderingene individuelle for hver behandling. Dermed vil ikke risikovurderingene leverandøren må foreta for å overholde GDPR kunne anvendes av en som ønsker å ta systemet i bruk. En risiko behandlingen utgjør for CV-eierne kan være legitim sett i lys av formålet med utviklingen av KI-systemet og samtidig ikke være det for en bedrift som ønsker å benytte seg av systemet for å effektivisere ansettelsesprosessen sin. Dette fører til at hovedaktørene må utføre flere risikovurderinger enn tidligere for å overholde begge regelverkene, noe som kan øke kostnadene og kompleksiteten ved implementering av AI Act.

5.3.2 Risikovurderinger før og under bruk av KI-systemet

I punkt 5.3.1 ovenfor ble risikovurderinger som må gjennomføres fra før et KI-system utvikles og frem til det er klart til å tilbys markedet behandlet. I likhet med etter GDPR

[182] Slike systemer vil som utgangspunkt klassifiseres som høyrisiko, se Rådets forslag fortalepunkt 36.
[183] Eksempelet er forenklet, men nyttig for illustrasjonens del. Rollefordelingen kan være annerledes. Eksempelvis finnes det regler om felles behandlingsansvar etter GDPR art. 26.

artikkel 35 er det også i AI Act lovfestet andre risiko-fokuserte legislative teknikker som ulike aktører må foreta og løpende oppdatere.[184] I denne delen vil fokuset ligge på Rådets forslag artikkel 9 som er nøkkelbestemmelsen for løpende risikostyring i forslaget.[185] Det er denne artikkelen som pålegger forpliktelser til de hovedaktørene oppgaven retter seg mot og som derfor er av relevans. Imidlertid kan det nevnes at artikkel 65 oppstiller forpliktelser til å utføre risikovurderinger for nasjonale myndigheter og at artikkel 71 om hvordan sanksjoner og straff skal bestemmes også gir uttrykk for en risiko-fokusert legislativ teknikk.[186]

Artikkel 9 ligger i forslagets del III kapittel 2 som inneholder forpliktelser for leverandøren av KI-systemet jf. Rådets forslag artikkel 16 nr. 1 bokstav a. Alle reglene i kapittel 2 har som formål å redusere risikoen høyrisiko KI-systemer utgjør.[187] AI Act antar imidlertid at selv om leverandøren overholder de øvrige kravene i kapittel 2 er ikke dette tilstrekkelig til å redusere all risiko til et akseptabelt nivå.[188] Formålet med artikkel 9 er å sørge for at leverandørene identifiserer de gjenstående risikoene og tar ytterligere grep for å redusere disse til et akseptabelt nivå.[189] Sett fra et slikt perspektiv er artikkel 9 en viktig backup hvor det åpnes opp for mer skjønnsmessige risikovurderinger fra leverandørens side enn AI Act for øvrig gjør, illustrert i punkt 4.2.

Rådets forslag artikkel 9 nr. 1 inneholder regler for når risikostyringssystemet skal etableres, mens i artikkel 9 nr. 2-7 utpensler hva det skal inneholde mer detaljert, herunder hvilke risikoer leverandøren skal vurdere. Begrepet risikostyringssystem er ikke legaldefinert i forordningen, men ordlyden i artikkel 9 nr. 8 tilsier at et risikostyringssystem er et slikt system som beskrevet i artikkelen nr. 1 til 7.[190]

Det følger av Rådets forslag artikkel 9 nr. 1 at et risikostyringssystem skal «be established, implemented, documented and maintained in relation to high-risk AI systems.». Videre følger det av artikkel 9 nr. 2 at dette systemet skal «be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating.». I likhet med en DPIA etter GDPR artikkel 35 er denne

---

[184] Tobias Mahler, «Between Risk Management and Proportionality: The Risk-Based Approach in the EU's Artificial Intelligence Act Proposal», *The Swedish Law and Informatics Research Institute*, 1 (2022), s. 247–270, på s. 252. [DOI: https://doi.org/10.53292/208f5901.38a67238] (lest 06.04.2023).
[185] Schuett (2023) s. 4.
[186] Mahler (2022) s 252.
[187] Schuett (2023) s. 4.
[188] Ibid.
[189] Ibid.
[190] Schuett (2023) s. 8.

risikovurderingsprosessen etter ordlyden gjentakende og krever systematisk oppdatering og oppfølging. Forpliktelsen foreligger kun for systemer som er høyrisiko etter AI Act. DPIA-prosessen foreligger derimot allerede om det er «sannsynlig» at behandlingen er høyrisiko etter GDPR. Selv om det følger indirekte av denne oppgaven er det viktig å poengtere at det som er høyrisiko i relasjon til AI Act ikke i alle tilfeller er høyrisiko i relasjon til GDPR og omvendt. Vurderingskriteriene er ulike og rekkevidden av regelverkene er ulikt.

Risikostyringssystemet består videre av to deler, risikostyringsprosessen jf. artikkel 9 nr. 2-4 og testingsprosedyrer jf. art. 9 nr. 5-7.[191] Risikostyringsprosessen skal skje gjennom hele livssyklusen til KI-systemet, jf. artikkel 9 nr. 2 gjennomgått ovenfor. Testingsprosedyren skal derimot skje under utviklingsprosessen frem til produktet når markedet jf. artikkel 9 nr. 7.[192]

Selv om AI Act ikke direkte gir rettigheter til enkeltindivider på samme måte som GDPR, er leverandøren nødt til å vurdere risikoen for fysiske personer som er utsatt for deres KI-system i risikostyringssystemet sitt.[193] Dette fremgår av ordlyden i artikkel 9 nr. 2 bokstav a som fastslår at første steg i risikostyringssystemet er å identifisere og analysere de kjente og forutsigbare risikoen for helse, sikkerhet og grunnleggende rettigheter i lys av det tiltenkte formålet med systemet. Det underbygges i fortalepunkt 42 at det er risikoen for helse, sikkerhet og de grunnleggende rettighetene til fysiske personer som skal være fokuset her. Det er ikke definert i bestemmelsen eller i Rådets forslag for øvrig hva som menes med kjente eller forutsigbare risikoer i lys av et høyrisiko KI-system. Ordlyden må derfor forstås slik at det er opp til leverandøren sitt skjønn å vurdere dette. En slik forståelse er også lagt til grunn i juridisk teori.[194] Leverandøren har dermed et friere skjønn under denne bestemmelsen enn etter AI Act for øvrig, noe som er mer likt den risikobaserte tilnærmingen i GDPR.

At leverandøren løpende må vurdere de grunnleggende rettighetene til individer som kan være utsatt for KI-systemet medfører at de må inn på noen av de samme vurderingene som behandlingsansvarlig/brukeren må inn på i sin DPIA etter GDPR artikkel 35. Personvern er, som nevnt, en av de grunnleggende rettighetene i EUs primærrett.[195] Når dette er tilfellet er det viktig at AI Act forsøker å harmonisere vurderingen foretatt av leverandøren etter AI Act

[191] Schuett (2023) s. 5.
[192] Dette kan i realiteten utvide rekkevidden til AI Act. Som gjennomgått under punkt 4. gjelder AI Act når systemet når det europeiske marked. For at denne testingsprosedyren skal kunne skje allerede under utvikling, må leverandøren kategorisere hvilken risikokategori systemet faller inn under før utvikling. Dette virker lite konsekvent.
[193] Schuett (2023) s. 8.
[194] Schuett (2023) s. 10.
[195] Se punkt 1.3.

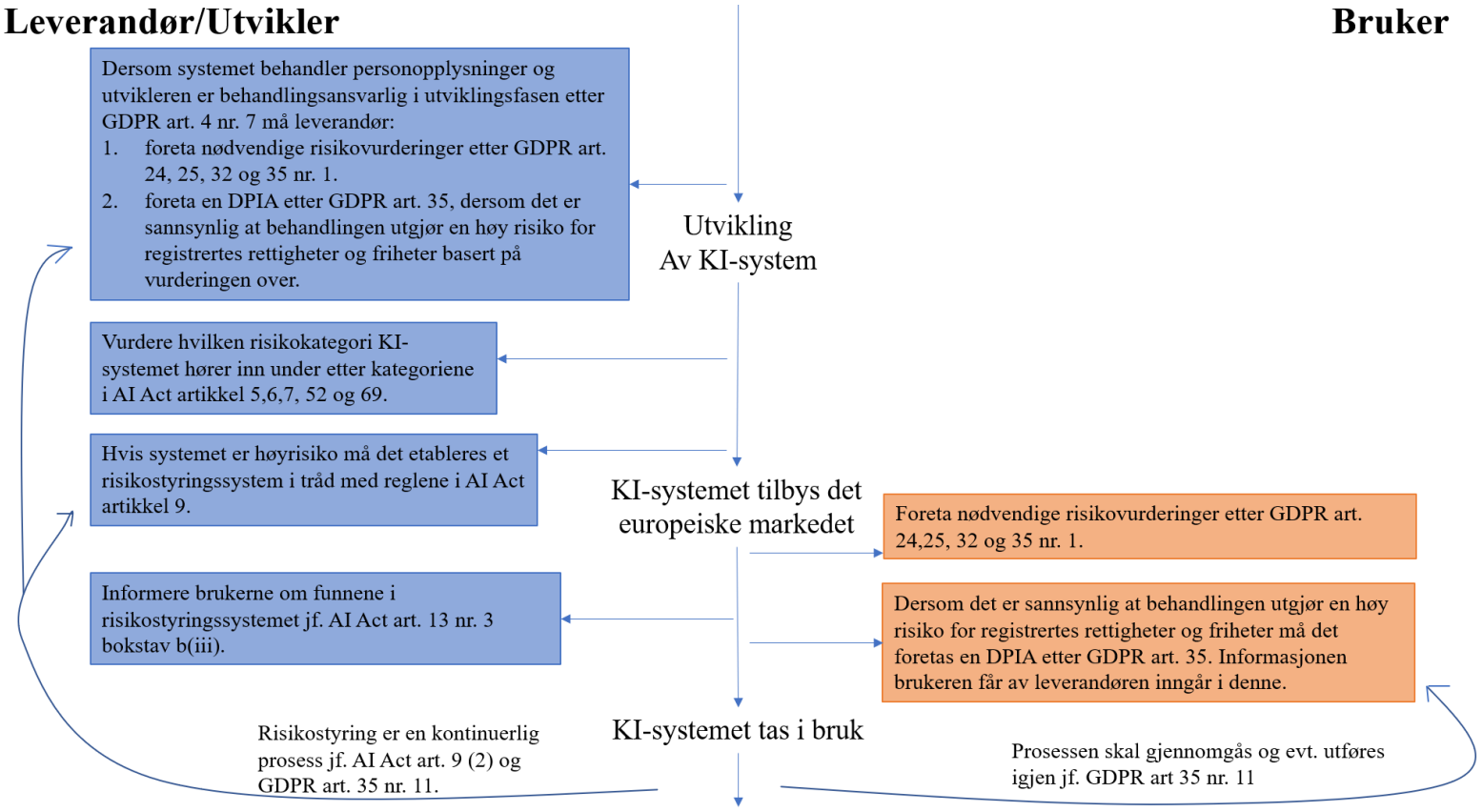
artikkel 9 og brukeren/behandlingsansvarlig etter GDPR artikkel 35. Det er både ressurskrevende og unødvendig om de to aktørene i praksis må foreta to lignende vurderinger uten å formidle funnene med hverandre. Dette poenget har Rådet sett. Dermed er det inntatt et krav i artikkel 13 nr. 3 bokstav b(iii) om at leverandøren må dele funnene sine etter artikkel 9 nr. 2 med brukeren av systemet, herunder hvilke situasjoner som det er kjent eller forutsigbart at kan utgjøre en risiko. Videre fremgår det av artikkel 29 nr. 6 at brukere av høyrisiko systemer skal bruke informasjonen de har fått av leverandøren etter artikkel 13 til å overholde forpliktelsen sin til å foreta en DPIA etter GDPR artikkel 35. At begge disse risikovurderingssystemene skal oppdateres løpende medfører at leverandøren løpende må oppdatere brukeren om sine funn i sitt risikovurderingssystem, slik at brukeren løpende kan oppdatere sin DPIA. Det er også oppstilt flere regler i AI Act om at brukeren må melde hendelser og gi andre tilbakemeldinger tilbake til leverandøren.[196] Samlet sett kommer overholdelse av GDPR artikkel 35 og AI Act artikkel 9 til å kreve et nært samarbeid mellom leverandøren og brukeren av KI-systemet. At den ene parten ikke gir tilstrekkelig med informasjon til den andre kan medføre at den andre risikerer å bryte sine forpliktelser etter ett eller begge regelverk.

Kommunikasjonen mellom leverandører og behandlingsansvarlige/brukere av KI-systemer er en utfordring allerede i dag. Dette kan forklares med at det frem til nå hovedsakelig har vært behandlingsansvarlig som har blitt ansvarliggjort for risikoen behandling av personopplysninger utgjør. Dermed har ikke databehandleren hatt det samme initiativet til å gi tilstrekkelig informasjon til behandlingsansvarlig. Der databehandler er tilknyttet et land utenfor EU har den vanskelige kommunikasjonen også kunnet forklares med at databehandler ikke har tilstrekkelig med kunnskap om hvilken informasjon behandlingsansvarlig trenger og hvorfor. Med AI Act vil også leverandøren/databehandler få et større risikoansvar og vil ha et større initiativ til å opprettholde en løpende, åpen og god kommunikasjon med brukeren. Dersom kommunikasjonen ikke er god nok risikerer også databehandler/leverandøren å sanksjoneres i større grad. Slik sett kan vedtakelsen av AI Act være med på å gjøre kommunikasjonen lettere.

[196] Se blant annet Rådets forslag art. 29 nr. 4.

5.3.3 Den samlede risikovurderingsprosessen

Sees funnene under punkt 5.3.1 og 5.3.2 samlet, kan det oppstilles en modell hovedaktørene i AI Act må følge for å overholde forpliktelsene til å foreta risikovurderinger etter de to regelverkene fullt ut i samspill med hverandre.



Figur 4: Risikovurderingsprosessen i GDPR og AI Act[197]

Modellen fokuserer utelukkende på risikovurderingene som må foretas. Det er en rekke andre forpliktelser hovedaktørene også må være bevisst. Eksempelvis faller noen av høyrisikosystemene etter Rådets forslag artikkel 6 under særlige kategorier av personopplysninger etter GDPR artikkel 9, se punkt 3.1. I disse tilfellene må brukeren/behandlingsansvarlige ha et ytterligere behandlingsgrunnlag for å ta systemet i bruk. Denne oppgaven avgrenser, som det fremgår av punkt 1.4.1, mot de øvrige aspektene hovedaktørene må være bevisst.

[197] Min egen illustrasjon. Bemerk at denne figuren vil se annerledes ut dersom det er slik at leverandøren må kategorisere systemet etter AIA allerede før utviklingen, se fotnote 192.

6. Avsluttende refleksjoner

Oppgaven har undersøkt hvordan risikovurderingene som må foretas etter AI Act samspiller med risikovurderingene som må foretas etter GDPR. Deretter har den redegjort for hvilke konsekvenser uklarheter og manglende harmonisering får for hovedaktørene under regelverkene.

Funn i oppgaven viser at den risikobaserte tilnærmingen i AI Act skiller seg betydelig fra den risikobaserte tilnærmingen i GDPR. Konsekvensene av dette er at det kan bli vanskelig å få et helhetlig bilde av risiko samt ansvaret risikoen medfører. Imidlertid har begge rettsaktene et felles mål om å ivareta EUs grunnleggende rettigheter og friheter, herunder retten til personvern. Ulikhetene i tilnærmingen til risiko kan dermed også medføre at risikoen samlet sett begrenses på en bedre måte og i større grad enn tidligere.

Videre er det flere av de konkrete kravene til risikovurderinger i AI Act som ikke er harmonisert med de allerede eksisterende kravene til risikovurderinger som må foretas etter bestemmelsene i GDPR kapittel IV. For å illustrere hvilke konsekvenser dette vil kunne få i praksis, har oppgaven redegjort for behandlingsansvarlig og databehandler etter GDPR. Deretter har leverandør og bruker under AI Act blitt behandlet og oppgaven har identifisert hvem disse er under GDPR. Funn i oppgaven viser at rollefordelingen i mange tilfeller endres i løpet av livsløpet til en KI og for ulike deler av en behandling, se punkt 5.3.

Dette har flere konsekvenser. For det første at det kan være vanskelig og ressurskrevende for hovedaktørene å forstå hvilken rolle de har i relasjon til de to regelverkene og følgelig hvilke forpliktelser de har og når. Videre må det utføres flere risikovurderinger enn de som allerede må gjennomføres etter GDPR. De fleste av disse kan neppe samordnes om det skal sikres full overholdelse av begge regelverk. Dette kommer til å medføre økte kostnader og kompleksiteten av overholdelse vil øke ytterligere utover hva som allerede er tilfellet etter GDPR. På den andre siden vil AI Act kunne bedre kommunikasjonen mellom behandlingsansvarlig og databehandler. Dette er fordi noe av risikoansvaret flyttes fra brukeren av et KI-system i sin rolle som behandlingsansvarlig etter GDPR og over til databehandleren i sin rolle som leverandør etter AI Act.

Avslutningsvis finnes det flere måter å begrense de negative konsekvensene på. En av disse er at nasjonale og internasjonale organer som har et helhetlig syn på regelverkene og evner å se

disse i sammenheng, lager gode veiledninger. Disse veiledningene må identifisere overlappende krav, mål, risikovurderinger og proporsjonalitetsvurderinger. På den måten vil de kunne trekke linjer til hvor informasjon innhentet etter kravene i den ene forordningen kan brukes til å overholde forpliktelsene etter den andre forordningen. Det er etter min mening ikke tilstrekkelig med organer som veileder bedrifter til overholdelse av ett av regelverkene isolert sett, slik som EDPB. Der regelverkene overlapper eller regulerer samme tilfelle, må veiledningene legge til rette for det. Eksempelvis kan dette gjøres ved å tilføye kapitler i veiledninger for overholdelse av AI Act om hva som må gjøres dersom KI-systemet behandler personopplysninger. I leverandørens veileder vil det da tilføyes en del der leverandøren bistås med å identifisere om vedkommende opptrer som databehandler eller behandlingsansvarlig i relasjon til GDPR. Dersom dette er tilfellet, bør det videre fremgå hvilke forpliktelser det medfører utover forpliktelsene etter AI Act.

Det samme gjelder brukeren. I veiledninger som lages for brukere i relasjon til AI Act bør det tilføyes en seksjon der brukere får hjelp til å identifisere om de er behandlingsansvarlig og hvilke forpliktelser dette gir etter GDPR. Gode modeller, figurer og andre verktøy vil være til hjelp i veiledningsprosessen. I figur 4 har jeg illustrert hvordan figurer kan brukes.

Videre må også pliktsubjektene selv sørge for at de har en helhetlig tilnærming til risikovurderingene som må foretas etter både GDPR og AI Act. Det er de som risikerer å sanksjoneres dersom de ikke overholder begge regelverk, og som derfor i første omgang har en økonomisk interesse i å ha en slik helhetlig tilnærming.

7. Litteraturliste

7.1 Norske lover og forarbeider

NOU 2022: 11	Ditt personvern – vårt felles ansvar. Tid for en personvernpolitikk.
Personopplysningsloven	Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven).

7.2 EU-rett

7.2.1 Traktater og konvensjoner

Charter of fundamental rights	Charter of Fundamental Rights of the European Union, 26. november 2012, 2012/C 326/02.
TEUV	Traktaten om Den europeiske unions virkeområde (TEUV), consolidated version of the Treaty on the Function of the European Union (TFEU), 26. november 2012, 2012/C 326/01.

7.2.2 Direktiver og forordninger

Forordning (EU) 2016/679 (GDPR)	Europaparlamentets- og Rådsforordning (EU) nr. 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) [GDPR].

7.2.3 Uttalelser, veiledninger og retningslinjer

A29, DPIA-retningslinje	«Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679», vedtatt 4. april 2017, som sist revidert og vedtatt 4. oktober 2017, WP 248 rev.01. Tilgjengelig her: https://ec.europa.eu/newsroom/article29/items/611236/en (lest 04.04.2023).
Council of the EU	«Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights», pressemelding, 6. desember 2022. Tilgjengelig her: Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights - Consilium (europa.eu) (lest 30.1.2023).
EDPB, Retningslinje 2/2019	«Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects», versjon 2, 8. oktober 2019. Tilgjengelig her: Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects | European Data Protection Board (europa.eu) (lest 5.2.2023).
EDPB, Retningslinje 4/2019	«Guidelines 4/2019 on Article 25 Data Protection by Design and by Default», versjon 1, 13. november 2019.

Tilgjengelig her: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en (lest 5.2.2023).

European Commission

«Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence», pressemelding, 21. april 2021.

Tilgjengelig her: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682 (lest 28.03.2023).

European Commission COM/2018/237

European Commission, «Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe», Brussel, 25. april 2018, COM/2018/237 endelig.

Tilgjengelig her: EUR-Lex - 52018DC0237 - EN - EUR-Lex (europa.eu) (lest 30.1.2023).

European Commission COM/2021/206

European Commission, «Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts», Brussel, 21. april 2021 COM/2021/206 endelig.

Tilgjengelig her: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 (lest 30.1.2023).

European Parliament	«Proposal for a Regulation on a European approach for Artificial Intelligence» i *A Europe Fit for the Digital Age*, Legislative train, 20. mars 2023. Tilgjengelig her: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence (lest 08.04.2023)
Independent High Level Expert Group set up by the European Commission	«Independent High Level Expert Group set up by the European Commission: A definition of AI: Main capabilities and diciplines», Brussel, 8. april 2019, B-1049. Tilgjengelig her: https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines (lest 5.2.2023).
OECD	«Recommendation of the Council on Artificial Intelligence», 22. mai 2019, OECD/LEGAL/0449. Tilgjengelig her: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#dates (lest 10.3.2023).

7.2.4 Rettspraksis fra EU-domstolen

Sak C-184/20	Dom av 1. august 2022 [GC], *OT v Vyriausioji tarnybinės etikos komisija,* C-184/20, ECLI:EU:C:2022:601.

7.3 Juridisk litteratur

7.3.1 Bøker

Fredriksen og Mathisen (2018) Fredriksen, Halvard Haukeland og Mathisen, Gjermund, *EØS-rett,* 3. utgave, Fagbokforlaget, 2018.

Gellert (2020) Gellert, Raphaël, *The risk-based approach to data protection*, 1. utgave, Oxford University Press, 2020.

Schartum (2020) Schartum, Dag Wiese, *Personvernforordningen – en lærebok*, 1. utgave, Fagbokforlaget, 2020.

Stemsrud (2016) Stemsrud, Odd, *EØS-rett i et nøtteskall,* 1. utgave, Gyldendal, 2016.

7.3.2 Artikler

Cofone (2019) Cofone, Ignacio N., «Algorithmic Discrimination Is an Information Problem», *Hastings Law Journal 70*, 3 (2019) s. 1389-1444.

Tilgjengelig her: https://www.hastingslawjournal.org/algorithmic-discrimination-is-an-information-problem/ (lest 14.03.2023).

De Gregorio og Dunn (2022) De Gregorio, Giovanni og Dunn, Pietro, «The European Risk-based Approaches: Connecting Constitutional Dots in the Digital Age», *Common Market Law Review 59*, 2 (2022) s. 473-500.

DOI: https://dx.doi.org/10.2139/ssrn.4071437.

Mahler (2022) Mahler, Tobias, «Between Risk Management and Proportionality: The Risk-Based Approach in the EU's

Artificial Intelligence Act Proposal», *The Swedish Law and Informatics Research Institute*, 1 (2022) s. 247–270.

DOI: https://doi.org/10.53292/208f5901.38a67238.

Schuett (2023) Schuett, Jonas, «Risk Management in the Artificial Intelligence Act», *European Journal of Risk Regulation,* First View (2023) s. 1-19.

DOI: https://doi.org/10.1017/err.2023.1.

7.3.3 Kommentarer og merknader

Eva Jarbekk (2021) Jarbekk, Eva. «Karnov lovkommentar til personvernforordningen.», i *Lovdata Pro* (2021) [lest 03.04.2023].

7.4 Andre kilder

7.4.1 Datatilsynet, departementene og andre offentlige organer

Datatilsynet Rapport, *Kunstig intelligens og personvern*, 11. januar 2018.

Tilgjengelig her: https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/kunstig-intelligens/ (lest 1.4.2023).

Datatilsynet «*Informasjonssikkerhet og internkontroll: Risikovurdering*», sist endret 16. juli 2019.

Tilgjengelig her:

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/risikovurdering/ (lest 15.03.2023).

Datatilsynet Rapport, «Finterai, sluttrapport: Maskinlæring uten datadeling», *Sandkasse for kunstig intelligens,* 11. oktober 2022.

Tilgjengelig her: https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/ferdige-prosjekter-og-rapporter/finterai-sluttrapport/veien-videre/ (lest 15.03.2023).

Datatilsynet «Biometri», sist endret 17. juli 2019.

Tilgjengelig her: https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/ (lest 31.03.2023).

Datatilsynet Veileder, *Vurdering av personvernkonsekvenser (DPIA)*, sist endret 17. juli 2019.

Tilgjengelig her: Veiledning om DPIA | Datatilsynet (lest 04.04. 2023).

Digdir «Ny forordning for kunstig intelligens», u.å.

Tilgjengelig her: Ny forordning for kunstig intelligens | Digdir (lest 07.03.2023).

Digdir «Om risiko og risikovurdering», u.å.

Tilgjengelig her: https://www.digdir.no/informasjonssikkerhet/om-risiko-og-risikovurdering/3048 (lest 15.03.2023).

Kommunal- og distriktsdepartementet	Norwegian Position Paper on the European Commission's Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021) 206), Norge, 4. August 2021, F2665314. Tilgjengelig her: Feedback from: Ministry of Local Government and Modernisation (europa.eu) (lest 10.03.2023).
Kommunal- og distriktsdepartementet	«Nasjonal strategi for kunstig intelligens», u.å. Tilgjengelig her: https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-kunstig-intelligens/id2685594/?ch=3 (lest 9.03.2023).
Kommunal- og distriktsdepartementet	«Forslag til forordning om kunstig intelligens (KI-forordningen)», EØS-notat, 21. juni. 2021, sist oppdatert 12. november 2021. Tilgjengelig her: Forslag til forordning om kunstig intelligens (KI-forordningen) - regjeringen.no (lest 30.4. 2023).
Utenriksdepartementet	«Slik blir EØS-regelverk til», sist endret den 21. mars 2023. Tilgjengelig her: https://www.regjeringen.no/no/tema/europapolitikk/eos1/eos-regelverk/id686837/ (lest 28.03.2023).

7.4.2 Internettadresser

Bertuzzi, Luca, «AI Act: European Parliament headed for key committee vote at end of April», *Euractive*, 30. mars 2023, oppdatert 31. mars 2023 [Tilgjengelig her: https://www.euractiv.com/section/artificial-intelligence/news/ai-act-european-parliament-headed-for-key-committee-vote-at-end-of-april/] (lest 08.04.2023).

Bertuzzi, Luca, «EU lawmakers set to settle on OECD definition for Artificial Intelligence», *Euractive*, 7. mars 2023, oppdatert 9. mars 2023 [Tilgjengelig her: EU lawmakers set to settle on OECD definition for Artificial Intelligence – EURACTIV.com] (lest 08.04.2023).

Bertuzzi, Luca, «MEPs seal the deal on Artificial Intelligence Act», *Euractive*, 27. april 2023, oppdatert 28. april 2023. [Tilgjengelig her: https://www.euractiv.com/section/artificial-intelligence/news/meps-seal-the-deal-on-artificial-intelligence-act/] (lest 03.05.2023).

Borgan, Eldrid, «Kunstig intelligens blir mannssjåvinistiske rasister. Hva kan vi gjøre for å stoppe det?», *Forskning.no*, 29. november 2019, [Tilgjengelig her: https://forskning.no/arbeid-it-juridiske-fag/kunstig-intelligens-blir-mannssjavinistiske-rasister-hva-kan-vi-gjore-for-a-stoppe-det/1599018] (lest 15.03.2023).

Edwards, Lilian, «The EU AI Act proposal», *Ada Lovelace Institute*, 2022 [Tilgjengelig her: Expert explainer: The EU AI Act proposal | Ada Lovelace Institute] (lest 10.3.2023).

Goswami, Rohan, «Bill Gates thinks A.I. like ChatGPT is the 'most important' innovation right now», *CNBC*, 10. februar 2023 [Tilgjengelig her: https://www.cnbc.com/2023/02/10/bill-gates-says-ai-like-chatgpt-is-the-most-important-innovation.html] (lest 17.03.2023).

Li, Xin, «Er dette fremtidens kunst?», *NRK*, 16. august 2022 [Tilgjengelig her: https://www.nrk.no/kultur/er-dette-fremtidens-kunst_-1.16048335] (lest 24.04.2023).

Morud, John Birger, «Ukraina bruker ansiktsgjenkjenning for å identifisere døde russiske soldater», *Forsvarets forum*, 4. april 2022 [Tilgjengelig her: https://forsvaretsforum.no/russland-ukraina/ukraina-bruker-ansiktsgjenkjenning-for-a-identifisere-dode-russiske-soldater/256609] (lest 24.04.2023).