Krysningspunktet mellom KI-forordningen og GDPR

KI-forordningens regulering av supplerende rettsgrunnlag for behandling av særlige kategorier av personopplysninger etter personvernforordningen

Kandidatnummer: 97

Antall ord: 14977

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10.12.2024

Innholdsfortegnelse

Innholdsfortegnelse 1
1 Innledning 3
1.1 Tema og fremstilling 3
1.2 Metode og rettskilder 5
1.3 Sentrale begreper 7
1.3.1 Personopplysningsbegrepet 7
1.3.2 Særlige kategorier 8
1.3.3 KI-system 10
1.4 Avgrensninger 11
2 GDPR 12
2.1 Introduksjon 12
2.2 Aktører 13
2.2.1 Behandlingsansvarlig 13
2.2.2 Databehandler 14
3 KI-forordningen 16
3.1 Introduksjon 16
3.2 Forbudte og høyrisiko KI-systemer 18
3.2.1 Forbudte KI-systemer 18
3.2.2 Høyrisiko KI-systemer 19
3.3 Aktører 20
3.3.1 Provider 20
3.3.2 Deployer 21
4 Krysningspunktet – GDPR og KI-forordningen 22
4.1 Behandling av personopplysninger 22
4.1.1 Behandlingsgrunnlag – utgangspunktet 22
4.1.2 Behandling av særlige kategorier av personopplysninger 23
4.2 KI-forordningen artikkel 10 (5) 24
4.2.1 Innledning 24
4.2.2 Nødvendig 26
4.2.3 Sikkerhets- og privatlivsbeskyttende tiltak 27
4.2.4 Konfidensialitet 29

4.2.5 Ikke blir oversendt 30
4.2.6 Sletting av personopplysninger 32
4.2.7 Begrunnelse i behandlingsprotokollene 33
4.2.8 Refleksjoner samt lovgivningsprosessen bak artikkel 10 (5) 34
4.3 KI-forordningen artikkel 59 38
4.3.1 Innledning 38
4.3.2 Offentlig interesse 39
4.3.3 Nødvendig 40
4.3.4 Overvåkningsmekanisme 41
4.3.5 Separat, isolert og beskyttet 42
4.3.6 Deling av data og personopplysninger 43
4.3.7 Valg overfor de registrerte 43
4.3.8 Tekniske og organisatoriske tiltak samt sletting 44
4.3.9 «Logs» over behandlingsaktivitetene 45
4.3.10 Beskrivelse av behandlingen 46
4.3.11 Kort sammenfatning 47
5 Avsluttende refleksjoner 48
6 Litteraturliste 51
6.1 Norsk rett 51
6.1.1 Norske lover og forarbeider 51
6.1.2 Forvaltningsorgan og tilsynsmyndigheter 51
6.2 EU-rett 53
6.2.1 Dommer fra EU-domstolen 53
6.2.2 Traktater og konvensjoner 54
6.2.3 Direktiver og forordninger 54
6.2.4 Lovforarbeid 55
6.2.5 Bindende beslutninger, uttalelser, veiledninger og retningslinjer 60
6.3 Juridisk litteratur 62
6.3.1 Bøker 62
6.3.2 Artikler 62
6.3.3 Lovkommentarer 63
6.4 Andre kilder 64
6.4.1 Internettadresser 64

1 Innledning

1.1 Tema og fremstilling

Tema for oppgaven er krysningspunktet mellom Artificial Intelligence Act (2024/1689/EU) («KI-forordningen») og General Data Protection Regulation (2016/679/EU) («GDPR»/«Personvernforordningen»). Oppgaven skal ta for seg sentrale personvernrettslige problemstillinger knyttet til krav som settes av KI-forordningen ved supplerende rettsgrunnlag for behandling av særlige kategorier av personopplysninger, og redegjøre for hvordan KI-forordningen og GDPR samvirker for å løse disse problemstillingene.

Forordningene er i utgangspunktet selvstendige. KI-forordningen regulerer bruken av KI-systemer uten at det nødvendigvis involverer personopplysninger,[1] og GDPR regulerer behandlingen av personopplysninger uten at det nødvendigvis involverer KI-systemer.[2] KI-forordningen har likevel enkelte bestemmelser som direkte bygger på eksisterende reguleringer i GDPR. Fokuset i denne oppgaven vil være på disse.

Især vil fokuset være på de supplerende rettsgrunnlagene i KI-forordningen som hjemler behandling av særlige kategorier[3] av personopplysninger etter GDPR – nemlig KI-forordningen artikkel 10 (5) og 59. Oppgaven skal undersøke hvorvidt kravene disse stiller for videre behandling av personopplysninger er hensiktsmessig utformet med tanke på det eksisterende personvernregelverket. Bestemmelsene tar henholdsvis for seg behandling av særlige kategorier av personopplysninger for skjevhetsoppdagelse og korrigering under trening, og for bruk i sandkasseeksperimenter.[4]

Disse bestemmelsene er valgt for å utforske krysningspunktet mellom forordningene, ettersom de bevisst bygger på den etablerte personvernsystematikken som følger av personvernforordningen.[5] Temaet treffer en rettslig kjerne ved bruken av kunstig intelligens, nemlig behandling av personopplysninger.

[1] For mer om personopplysningsbegrepet, se punkt 1.3.1.
[2] For mer om KI-systembegrepet, se punkt 1.3.3, for virkeområdene generelt, se henholdsvis kapittel 3 og 2.
[3] For mer om særlige kategorier av personopplysninger, se punkt 1.3.2.
[4] Dette vil bli redegjort for nærmere i punkt 4.2 og 4.3.
[5] Bestemmelsene vil utdypes i kapittel 4.

KI-forordningen, som er det første regelverket i verden som særskilt regulerer bruken av kunstig intelligens,[6] ble vedtatt av EU-parlamentet den 13. mars 2024.[7] Forordningen trådte delvis i kraft allerede 1. august 2024.[8] Ettersom KI-forordningen ennå er i en tidlig fase som EU-forordning – med flere bestemmelser som ikke har trådt i kraft –[9] har en rekke rettslige problemstillinger ikke blitt satt på spissen, og er dermed per nå uutforsket. Særlig ligger den personvernrettslige problematikken latent. KI-systemer er trent på, får inn og gir ut store mengder data. At KI-systemer da enten bevisst, ubevisst, direkte eller indirekte involveres med personopplysninger, er nærmest gitt.

Eksempelvis har enkelte opplevd at personopplysninger om seg selv – som e-poster – har blitt gitt direkte til brukere av generative KI-modeller som ChatGPT.[10] Slike tilfeller har ført til skepsis over hvor godt KI-systemene ivaretar personvernet. Enkelte personvereksperter anser KI-modellene for å være personvernrettslig «råtne ved fundamentet», og anklager utviklerne bak KI-modeller som ChatGPT for å ha utviklet disse uten innebygd personvern eller personvern som standard.[11]

Innebygd personvern og personvern som standard er generelle krav som GDPR stiller ved enhver behandling av personopplysninger.[12] Leverandører av KI-systemer har dermed vanskeligheter med å følge og etterleve selv det eksisterende personvernregelverket med alle dets rettigheter og krav. I forlengelsen av dette kan det særlig problematiseres hvordan de *nye* lovreguleringene i KI-forordningen står seg i henhold til det eksisterende personvernregelverket, og om lovgiver har tilstrekkelig hensyntatt etterlevelsesproblematikken. Når KI-forordningen i enkelte situasjoner åpner opp for viderebehandling av særlige kategorier av personopplysninger,[13] slik som etter KI-forordningen artikkel 10 (5) og 59, blir problemstillingen særlig aktuell. Især om denne adgangen er gjort på en måte som lovteknisk

[6] Det Europeiske parlament, «Artificial Intelligence Act: MEPs adopt landmark law», *Det Europeiske parlament*, 13 mars 2024 [Tilgjengelig: https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law] (lest 15.08.2024).
[7] Ibid.
[8] KI-forordningen artikkel 113.
[9] Ibid.
[10] Jeremy White, «How Strangers Got My Email Address From ChatGPT's Model», *The New York Times*, 22. desember 2023 [Tilgjengelig: https://www.nytimes.com/interactive/2023/12/22/technology/openai-chatgpt-privacy-exploit.html] (lest 16.08.2024).
[11] Matt Burgess, «ChatGPT Has a Big Privacy Problem», *Wired*, 4. april 2023 [Tilgjengelig: https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/] (lest 15.08.2024).
[12] For mer om de generelle kravene, se punkt 2.1.
[13] Dette vil utdypes i kapittel 4.

passer sømløst inn med de eksisterende forpliktelsene og lovsystematikken som følger av personvernforordningen. Eventuelt om det foreligger spenning.

KI-forordningen er i utgangspunktet utformet slik at den er ment å kunne anvendes side om side med GDPR. Dette fremkommer av KI-forordningen artikkel 2 (7), hvor det stadfestes at «[t]his Regulation shall not affect [GDPR]», med unntak av nettopp overnevnte artikkel 10 (5) og 59. Hvorvidt dette faktisk stemmer, og hvor godt disse bestemmelsene harmoniserer med det eksisterende personvernregelverket, vil analyseres i kapittel 4. Videre i kapittel 1 vil de mest sentrale aspektene ved oppgaven redegjøres for, før det i kapittel 2 og 3 vil redegjøres for henholdsvis GDPR og KI-forordningen. Avslutningsvis i kapittel 5 vil krysningspunktet mellom GDPR og KI-forordningen og bestemmelsenes lovtekniske egnethet kommenteres i lys av det analyserte.

1.2 Metode og rettskilder

Både KI-forordningen og GDPR er begge vedtatte EU-forordninger, og offentliggjort i Den europeiske unions tidende.[14] EU-forordninger er i utgangspunktet ikke norsk rett, men blir en del av den norske rettsordenen ved å bli innlemmet i EØS-avtalen og deretter gjennomført i nasjonal rett.[15] Mens GDPR har vært en del av EØS-avtalen siden 6. juli 2018,[16] er KI-forordningen ennå ikke blitt innlemmet og gjort til en del av norsk rett.[17] Norske myndigheter har likevel gitt klare signaler om at KI-forordningen er ønsket inn i EØS-avtalen, og at den skal bli en del av den interne norske rettsordenen.[18]

Ved tolkningen av EU-rettsakter vil utgangspunktet være – uavhengig om de er innlemmet i EØS-avtalen eller ei – tolkningsprinsippene slik de er utviklet av EU-domstolen.[19] Videre vil homogenitetsprinsippet tilsi at forordninger som er inntatt i norsk rett gjennom EØS-avtalen,

[14] Tilgjengelig på https://eur-lex.europa.eu/eli/reg/2024/1689/oj og https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[15] Fredriksen og Mathisen (2022), s. 390–391.
[16] EØS-komiteens besl. nr. 154/2018 og EØS-tillegget til Den europeiske unions tidende Nr. 46 25. årgang 19.7.2018.
[17] Regjeringen, «Forslag til forordning om kunstig intelligens (KI-forordningen)», *Regjeringen.no*, 29. januar 2024 [Tilgjengelig: https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/juni/forslag-til-forordning-om-kunstig-intelligens-ki-forordningen/id2884935/] (lest 19.08.2024).
[18] Kommunal- og moderniseringsdepartementet – Holdningsdokument KI-forordningen, s. 1.
[19] Fredriksen og Mathisen (2022), s. 328.

skal tolkes likt som i resten av EU.[20] Rettspraksis fra EU-domstolen på personvernrettsfeltet vil dermed være sentral i den videre juridiske analysen ved tolkningen av de to EU-forordningene.

Veiledninger, retningslinjer og anbefalinger som tar for seg lovspørsmål angående GDPR vil også stå sentralt. Personvernrådet («EDPB») ble opprettet da GDPR ble vedtatt, jfr. GDPR artikkel 68 (1), og har etter GDPR artikkel 70 muligheten til å på eget initiativ å komme med retningslinjer, anbefalinger og beste praksis. Disse er ikke bindene, men blir tillagt stor vekt.[21] EDPBs mål er å sikre «ensartet anvendelse» av GDPR,[22] og står derfor sentral ved tolkningen av vilkår etter GDPR. EDPB har kommet med en rekke veiledninger og retningslinjer som tar for seg sentrale deler av personvernretten, og har også tilsluttet seg en rekke retningslinjer fra den eldre WP29-gruppen,[23] som ble satt opp av artikkel 29 under det gamle personverndirektivet.[24] Veiledningene har også blitt vektlagt i norsk forvaltning, da særlig av personvernnemda, eksempelvis i PVN-2022-22, men òg av det norske datatilsynet, som i PVN-2021-20. I den juridiske analysen vil derfor uttalelser av EDPB gitt i kraft av GDPR artikkel 70 vektlegges for å utpensle og tolke lovbestemmelser.

Det norske datatilsynet («Datatilsynet») er etter GDPR artikkel 51 og personopplysningsloven[25] § 20 den utnevnte tilsynsmyndigheten i Norge. Datatilsynet har etter GDPR artikkel 57 (1) bokstav b som oppgave å fremme allmennhetens kunnskap rundt forordningen. Datatilsynet har i lys av dette kommet med veiledninger og uttalelser angående anvendelsen av regelverket.[26] Datatilsynet har videre en plikt etter GDPR artikkel 57 (1) bokstav i til å «følge relevant utvikling, i den grad den har innvirkning på personvern, særlig utviklingen innen informasjons- og kommunikasjonsteknologi og handelspraksis». Denne plikten har munnet ut i at Datatilsynet har kommet med en rekke uttalelser angående KI, KI-forordningen og dens skjæringspunkt med GDPR.[27] Disse uttalelsene vil følgelig også tas i betraktning for å belyse de GDPR-rettslige problemstillingene som reises ved krysningspunktet med KI, ettersom Datatilsynet har inngående kunnskap og erfaring innenfor personvernsfeltet.

[20] EØS-avtalen artikkel 6 og ODA artikkel 3 (2), se også Fredriksen og Mathisen (2022), s. 258.
[21] Prop. 56 LS (2017–2018) s. 168.
[22] GDPR artikkel 70 (1).
[23] European Data Protection Board, «Endorsed WP29 Guidelines», *edpb.europa.eu* [Tilgjengelig: https://www.edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en] (lest 20.08.2024).
[24] Direktiv 95/46/EF.
[25] Lov 15. juni 2018 nr. 38 om behandling av personopplysninger.
[26] Tilgjengelige på https://www.datatilsynet.no/.
[27] Datatilsynet – «Kunstig intelligens og personvern».

1.3 Sentrale begreper

1.3.1 Personopplysningsbegrepet

Med *personopplysninger* menes «enhver opplysning om en identifisert eller identifiserbar fysisk person («*den registrerte*»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator […]»,[28] jfr. GDPR artikkel 4 (1). Begrepet står sentralt i personvernforordningen, og utgjør hovedskillet mellom hvilke typer opplysninger som omfattes og hvilke som *ikke* omfattes av GDPR. Slik ordlyden «enhver opplysning» og «identifiserbar» tilsier, favner personopplysningsbegrepet svært vidt.

Begrepet «enhver opplysning» er ikke begrenset til sanne opplysninger, men omfatter også falske opplysninger.[29] Subjektive opplysninger omfattes også, slik at vurderinger om fysiske personer faller inn under personopplysningsbegrepet.[30] Begrepet omfatter også «direkte eller indirekte» opplysninger.[31] Dersom en opplysning om en gjenstand indirekte kan knyttes opp mot en person, som gjør det mulig å identifisere vedkommende, vil opplysningen fanges opp av personopplysningsbegrepet. Dette kan for eksempel være et bilskilt. En avgrensning er imidlertid at døde personer ikke omfattes.[32] Den vide ordlyden «enhver opplysning» er som poengtert av EU-domstolen til for å nettopp reflektere «[…] the aim of the EU legislature to assign a wide scope to that concept».[33]

Et eksempel på hvor langt ordlyden rekker er *IAB Europe [C5]* C-604/22, hvor en rekke bokstav- og tegnkombinasjoner som inneholdt en brukers samtykkepreferanse ble ansett å utgjøre personopplysninger. Det var nemlig *mulig* å knytte disse opp til en identifikator, for eksempel en IP-adresse, hvilket lot den registrerte bli identifisert med en preferanse. Dette da selv om den behandlingsansvarlige[34] *ikke* hadde identifikatoren.[35] Med andre ord kan personopplysningsbegrepet tåle store avstander med mange – faktiske og teoretiske – steg mellom et stykke informasjon og den registrerte, og likevel gjøre seg gjeldende med full styrke.

---

[28] Min kursivering.
[29] Artikkel 29-gruppen – Uttalelse 4/2007 (2007), s. 6.
[30] Ibid.
[31] Ibid.
[32] Se GDPR fortalepunkt 27.
[33] *Pankki S [C5]* C-579/21 avsnitt 42.
[34] Se punkt 2.2.1 for behandlingsansvarligbegrepet.
[35] *IAB Europe [C5]* C-604/22 avsnitt 40 og 46, mens EU-domstolen mente på avsnitt 48–49 at databehandleren kunne få adgang til denne identifikatoren, ble det eksplisitt stadfestet i de førstnevnte avsnittene at dette ikke var avgjørende.

En begrensning slik det følger av GDPR fortalepunkt 26, er imidlertid at det skal tas «hensyn til alle midler som det med *rimelighet* kan tenkes at […] en annen person kan ta i bruk for å identifisere vedkommende direkte eller indirekte».[36] Hva som derimot er rimelig vil variere i stor grad ut fra hvilken situasjon en står overfor. Som påpekt på avsnitt 36 i den overnevnte dommen, kan personopplysningsbegrepet altså da «[…] potentially encompass[] all kinds of information […]».

Personopplysninger kan videre deles inn i to kategorier: alminnelige personopplysninger, og særlige kategorier av personopplysninger. Alminnelige personopplysninger – som ikke defineres i GDPR, men er hensiktsmessig å benytte seg av – vil brukes heretter for å beskrive enhver personopplysning som ikke faller inn under en særlig kategori. Særlige kategorier av personopplysninger vil redegjøres for i det følgende. Ved anvendelsen av KI-forordningen skal personopplysningsbegrepet forstås likt som etter GDPR, jfr. KI-forordningen artikkel 2 (50).

1.3.2 Særlige kategorier

Hva som utgjør *særlige kategorier* av personopplysninger defineres i GDPR artikkel 9 (1), og er personopplysninger om:

> *[…] rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.*

Listen er uttømmende.[37] De ulike kategoriene tolkes likevel vidt. I *OT [GC]* C-184/20 tolket EU-domstolen GDPR artikkel 9 (1) slik at personopplysninger som er «liable to disclose indirectly the sexual orientation of a natural person», må anses å utgjøre særlige kategorier av personopplysninger. I den saken ble dermed publiseringen av navnet til den registrertes samboer anset å være en behandling av særlige kategorier av personopplysninger, ettersom det var mulig å dedusere vedkommendes seksuelle legning. At GDPR forutsetter en vid tolkning, ble lagt eksplisitt til grunn av EU-domstolen på avsnitt 125. Fotografier er likevel ikke

[36] Min kursivering.
[37] Kuner mfl. (2020), s. 373.

automatisk ansett som særlige kategorier av personopplysninger, selv om slikt følgelig kan inneholde opplysninger om f.eks. «etnisk opphav».[38]

De overnevnte kategoriene av personopplysninger anses å være av en særlig *sensitiv* natur. Kategoriene ble omtalt som nettopp slikt i fortalen til det tidligere personverndirektivet (95/46/EF),[39] og tilsvarende legaldefinert i den gamle personopplysningsloven[40] § 8 nr. 2. Disse personopplysningene er i utgangspunktet forbudt å behandle.[41] Forbudet tolkes strengt, og EU-domstolen har i eksempelvis *Meta Platforms Inc [GC]* C-252/21 på avsnitt 69 stadfestet at forbudet mot behandling av særlige kategorier av personopplysninger gjelder uavhengig om opplysningene er sanne, eller om den behandlingsansvarlige har ment å behandle dem.

Behandlingsforbudet er imidlertid ikke absolutt. GDPR artikkel 9 (2) legger frem en uttømmende liste med alternative vilkår som, hvis oppfylt, opphever forbudet i første ledd og åpner opp for at den behandlingsansvarlige likevel kan behandle slike opplysninger. Eksempler på slike unntak er uttrykkelig samtykke fra den registrerte, at det er åpenbart at personopplysningene er offentliggjort av den registrerte, om behandlingen er nødvendig for å verne noens vitale interesser hvor den registrerte ikke er i stand til å gi samtykke, eller nødvendig av hensyn til allmenne interesser med grunnlag i lov.[42] Sistnevnte unntak vil utforskes ytterligere i punkt 4.1.2, og står i kjernen av oppgavens analyse av KI-forordningen artikkel 10 (5) og 59.

[38] Se GDPR fortalepunkt 51.
[39] Primært i den engelske språkversjonen, i den norske oversettelsen av fortalen oversatt som «følsomme opplysninger», jfr. Personverndirektivet fortalepunkt 34 og 70.
[40] Lov 14. april 2000 nr. 31 om behandling av personopplysninger.
[41] GDPR artikkel 9 (1).
[42] Se henholdsvis GDPR artikkel 9 (2) bokstav a, e, c, og g.

1.3.3 KI-system

I KI-forordningen er det KI-systemene som står sentralt. Et *KI-system* defineres etter KI-forordningen artikkel 3 (1) som et:

> *[…] machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.*

Legaldefinisjonen tar for seg mange fasetter for å definere kunstig intelligens. Dette er nødvendig for å både være teknologisk fleksibel og for å fange opp utviklingene og kompleksitetene rundt KI-systemer, samt for å utelukke andre «enklere» datasystemer som ikke naturlig hører inn under KI-begrepet.[43] Definisjonen er videre utformet for å være i samsvar med internasjonale organisasjoners arbeid med kunstig intelligens.[44]

KI-forordningen legger til grunn at noe av det som skiller KI-systemer fra andre systemer, er deres evne til å trekke slutninger.[45] Evnen til å trekke slutninger hever KI-systemene over grunnleggende databehandling ved å muliggjøre læring, resonnering eller modellering.[46] Videre er et kjennetrekk ved KI-systemer at de er tiltenkt å fungere med varierende grad av selvstendighet. Det er særlig ved «input[s]» og genererte «outputs» at de personvernrettslige problemstillingene aktualiserer seg hos KI-systemene. Slik det vil redegjøres for i kapittel 4, kan de også oppstå i treningsfasen og i andre særlige KI-situasjoner hvor personopplysninger behandles.

[43] Se KI-forordningen fortalepunkt 12.
[44] Ibid.
[45] Ibid. (EN/DK/SE: to infer/at udlede/dra slutsatser).
[46] Ibid.

1.4 Avgrensninger

Personopplysningsregelverket og KI-forordningen har flere krysningspunkter enn dem som vil bli fremhevet i denne oppgaven. Tilnærmet all bruk av kunstig intelligens vil ha et personvernrettslig tilsnitt.[47] Det vil dermed være lite hensiktsmessig å ta for seg samtlige problemstillinger, eller å ta for seg problemstillingene på et for generelt og abstrakt nivå. Eksempelvis vil dette være KI-systemer som tar automatiserte avgjørelser basert på personopplysninger, hvilket reguleres av GDPR artikkel 22. Denne og lignende problemstillinger er høyaktuelle, men går utover denne oppgaven.

Oppgaven avgrenses derfor mot øvrige personvernrettslige problemstillinger som oppstår ved bruk av KI, og vil utelukkende problematisere de personvernrettslige problemstillingene som oppstår hvor KI-forordningen konkret og bevisst henviser og bygger på det eksisterende personvernregelverket slik det følger av GDPR. Som tidligere nevnt, vil dette være KI-forordningen artikkel 10 (5) og 59. Ettersom EU-lovgiver som poengtert i punkt 1.1 har åpnet opp for at disse bestemmelsene kan modifisere det eksisterende personvernregelverket, er det av særlig interesse å se om dette har skjedd på en lovteknisk hensiktsmessig måte – eventuelt om én av disse artiklene gjør dette bedre enn den andre.

Det avgrenses også mot å redegjøre for andre aspekter ved KI-forordningen som ikke har et personvernrettslig tilsnitt. Aktører, kategorier og øvrige reguleringer i KI-forordningen vil bli redegjort for i den grad det er nødvendig for å forstå anvendelsen og bakgrunnen for KI-forordningen artikkel 10 (5) og 59, og den generelle systematikken i KI-forordningen.

[47] Hovedsakelig på grunn av det vide nedslagsfeltet til personopplysningsbegrepet, se punkt 1.3.1.

2 GDPR

2.1 Introduksjon

Personvernforordningen er det fremste regelverket som regulerer behandlingen av personopplysninger i EU/EØS,[48] og sammen med personopplysningsloven, også i Norge. Formålet med forordningen er å fastsette regler som både verner om fysiske personer i forbindelse med behandling av personopplysninger, samt fri utveksling av personopplysninger.[49] Forordningen får anvendelse på automatiserte og ikke-automatiserte behandlinger av personopplysninger som er eller skal inngå i et register.[50] Forordningen er utformet teknologinøytralt. Den vil derfor omfatte bruk av personopplysninger i KI-systemer, så vel som andre enklere former for teknologiske personopplysningsbehandlingssystem, som manuell behandling.[51]

GDPR setter en rekke *vilkår og krav* for at en skal kunne behandle personopplysninger, samt gir den registrerte – den det behandles personopplysninger om –[52] en rekke *rettigheter* som vedkommende kan påberope seg i kraft av forordningen. Av vilkår foreligger det blant annet krav om at det foreligger et behandlingsgrunnlag,[53] krav om innebygd personvern og personvern som standard,[54] og krav om at den behandlingsansvarlige[55] og databehandleren[56] skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et egnet sikkerhetsnivå.[57] Av rettigheter har den registrerte blant annet rett til retting og sletting,[58] til å bli informert,[59] til innsyn i – og å få kopi av – ens egne personopplysninger,[60] m.m. GDPR stiller dermed opp et regulatorisk rammeverk som overordnet og systematisk gjennom vilkår og håndhevbare rettigheter er tiltenkt å verne om enkeltindividers personopplysninger.

[48] Men ikke eneste, se f.eks. 2018/1725/EU («EUDPR»).
[49] GDPR artikkel 1 (1).
[50] GDPR artikkel 2 (1).
[51] GDPR fortalepunkt 15.
[52] Se punkt 1.3.1 for definisjonen av den registrerte.
[53] GDPR artikkel 6.
[54] GDPR artikkel 25.
[55] Se punkt 2.2.1 for behandlingsansvarligbegrepet.
[56] Se punkt 2.2.2 for databehandlerbegrepet.
[57] GDPR artikkel 32.
[58] GDPR artikkel 16 og 17.
[59] GDPR artikkel 13.
[60] GDPR artikkel 15.

GDPR er altså hovedsakelig en rettighetsforordning, og er ment å være en regulatorisk konkretisering av hvordan personopplysninger juridisk skal vernes,[61] og som sikrer et ensartet og høyt nivå av personvern for fysiske personer – de registrerte.[62] Retten til vern av personopplysninger er nedfelt i Den europeiske unions pakt om grunnleggende rettigheter artikkel 8 (1) og i artikkel 16 (1) i traktaten om Den europeiske unions virkemåte («TEUV»).[63] Personvernet utgjør dermed en grunnpilar blant de fundamentale rettighetene i EU-retten. Foruten den registrerte,[64] er den behandlingsansvarlige og databehandlerne helt sentrale aktører i personvernforordningen, og som sammen med den registrerte legger til rette for anvendelsen og håndhevelsen av personvernregelverket. Disse aktørene er viktige for å forstå systematikken i GDPR og vil i det følgende redegjøres for.

2.2 Aktører

2.2.1 Behandlingsansvarlig

Den behandlingsansvarlige er etter GDPR den som «alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes», jfr. GDPR artikkel 4 (7). Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at forordningens grunnleggende prinsipper overholdes,[65] herunder at behandlingen er *lovlig*.[66] Denne plikten omtales som ansvarlighetsprinsippet. Den behandlingsansvarlige har i lys av dette et ansvar for å sørge for at behandlingen alltid har et behandlingsgrunnlag.[67] Foreligger det ikke et behandlingsgrunnlag, anses ikke behandlingen som lovlig. Dette strider med grunnprinsippene,[68] og kan sanksjoneres med overtredelsesgebyrer.[69] Den behandlingsansvarlige pålegges som hovedpliktsubjekt en rekke forpliktelser etter forordningen gjennom ansvarlighetsprinsippet,[70] og står som hovedansvarlig overfor den

[61] GDPR artikkel 1 (2).
[62] GDPR fortalepunkt 10.
[63] GDPR fortalepunkt 1.
[64] Se punkt 1.3.1 for definisjonen av den registrerte.
[65] GDPR artikkel 5 (2).
[66] GDPR artikkel 5 (1) bokstav a.
[67] Se punkt 4.1 for behandlingsgrunnlagsbegrepet.
[68] GDPR artikkel 5 (1) bokstav a og artikkel 6 (1).
[69] GDPR artikkel 83 (5) bokstav a.
[70] Som redegjort for i punkt 2.1.

registrerte ved brudd og krenkelser.[71] Rollen som behandlingsansvarlig står følgelig sentral i personvernforordningen.

Behandlingsansvarligbegrepet er funksjonelt. Det er den som *faktisk* bestemmer formålet som anses som behandlingsansvarlig, og er derfor uavhengig av eventuelle privatrettslige avtaler som utpeker noen som behandlingsansvarlig.[72] Kontraktsrettslige reguleringer kan likevel bidra med å avgjøre hvem som skal anses som behandlingsansvarlig.[73]

Begrepet er utformet funksjonelt for å unngå situasjoner hvor en ikke klarer å utpeke en behandlingsansvarlig, og skal dermed tolkes såpass bredt at en unngår gap i rollefordelingen hvor ingen ansvarliggjøres for brudd på forordningen.[74] Dette vil også forhindre at en behandlingsansvarlig prøver å avtale seg vekk fra rollen som behandlingsansvarlig for å unngå plikter. At en ikke har *ment* å behandle personopplysninger, er irrelevant for hvorvidt en skal anses som behandlingsansvarlig eller ei.[75]

2.2.2 Databehandler

En databehandler er en som «behandler personopplysninger på vegne av den behandlingsansvarlige», jfr. GDPR artikkel 4 (8). En databehandler pålegges også plikter etter personvernforordningen, men ansvaret er begrenset.[76] Dette er fordi databehandlere ikke har et eget behandlingsgrunnlag, men utleder sin rett til å behandle personopplysninger gjennom en databehandleravtale med den behandlingsansvarlige.[77] Et viktig ansvar er likevel at databehandleren ikke bare, som nevnt i punkt 2.1, skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et egnet sikkerhetsnivå.[78] Databehandleren skal også gi den behandlingsansvarlige *tilstrekkelige garantier* for at de vil gjøre dette.[79]

---

[71] Kuner mfl. (2020), s. 146, og Skullerud mfl. (2023), Artikkel 4. Definisjoner, Juridika [Tilgjengelig: https://juridika.no/lov/2016-04-27-679/%C2%A74/kommentar/] (lest 28.08.2024).
[72] EDPB – Retningslinje 07/2020, avsnitt 12.
[73] Ibid. avsnitt 26.
[74] Ibid. avsnitt 14.
[75] Ibid. avsnitt 41.
[76] Skullerud mfl. (2023), Artikkel 4. Definisjoner, Juridika [Tilgjengelig: https://juridika.no/lov/2016-04-27-679/%C2%A74/kommentar/] (lest 28.08.2024).
[77] GDPR artikkel 28 (3).
[78] GDPR artikkel 32 (1).
[79] GDPR artikkel 28 (1).

Det sentrale er at databehandleren behandler personopplysninger på vegne av den behandlingsansvarlige, og da etter dens dokumenterte instrukser.[80] Dersom en databehandler begynner å behandle personopplysninger for andre formål enn det som er satt av den behandlingsansvarlige, anses databehandleren selv som behandlingsansvarlig.[81] Dette skyldes at databehandleren, ved å avvike fra den opprinnelige behandlingsansvarliges instruksjoner, blir den som i realiteten – funksjonelt –[82] bestemmer formålet med behandlingen av personopplysninger. Databehandleren blir da underlagt alle forpliktelsene etter GDPR som påhviler den behandlingsansvarlige.[83]

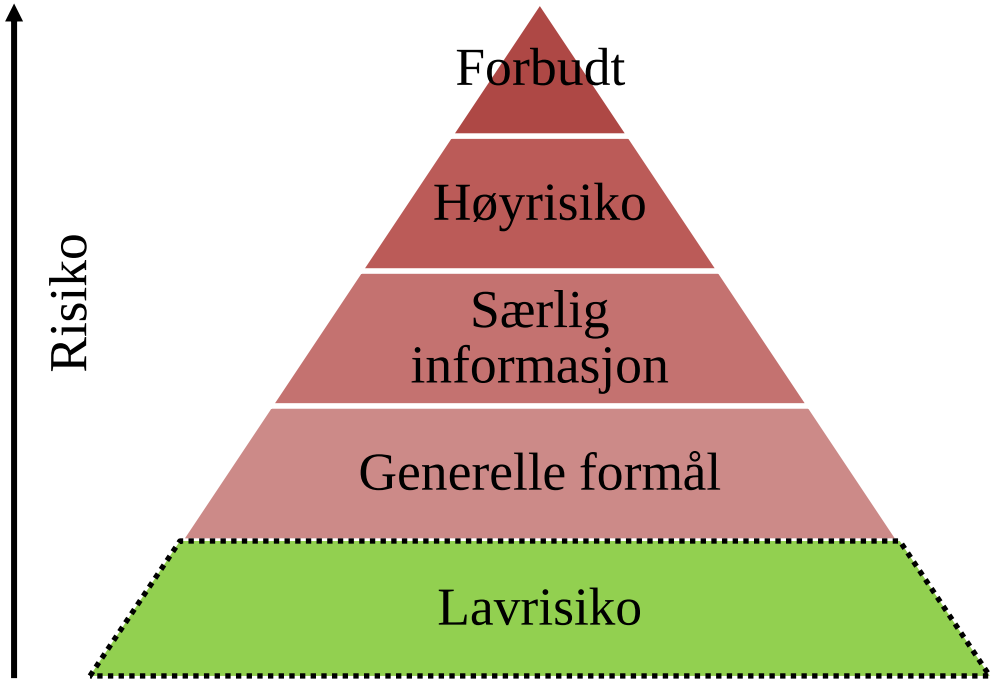
Databehandlere utgjør en sentral rolle i personvernrettssfæren, og blir hyppig brukt av behandlingsansvarlige for å behandle personvernopplysninger på deres vegne. Tjenester som eksempelvis skylagring faller ofte inn under databehandlerbegrepet, ettersom skytjenesten lagrer – og dermed behandler –[84] personopplysninger på vegne av den behandlingsansvarlige. De færreste behandlingsansvarlige som behandler personopplysninger i en stor skala, eller for kommersielle formål, behandler dermed personopplysninger uten å benytte seg av en databehandler.

[80] GDPR artikkel 29 og 28 (3).
[81] GDPR artikkel 28 (10).
[82] Se punkt 2.2.1 for behandlingsansvarligbegrepet.
[83] Se punkt 2.2.1 for forpliktelsene som påhviler den behandlingsansvarlige.
[84] GDPR artikkel 4 (2).

3 KI-forordningen

3.1 Introduksjon

KI-forordningen er, som nevnt i punkt 1.1, i en verdenssammenheng den første av sitt slag. KI-forordningen er tiltenkt å regulere sikkerheten rundt kunstig intelligens som er tilgjengelig på det indre markedet,[85] men også å verne om EU-borgernes grunnleggende rettigheter og helse.[86] KI-forordningen har hovedsakelig en risikobasert tilnærming til reguleringen av KI, og deler KI-systemene opp deretter.[87] KI-forordningen definerer risiko som «the combination of the probability of an occurrence of harm and the severity of that harm».[88] KI-forordningen deler KI-system opp i fem forskjellige kategorier, alt etter hvor stor risiko KI-systemet utgjør. De fem kategoriene er: forbudt KI som har uakseptabel risiko,[89] KI med høy risiko,[90] KI som krever særlig informasjon,[91] KI med generelle formål,[92] og KI med lav risiko. KI-systemer som har lav risiko, særreguleres ikke av forordningen.[93] Kategoriene kan enkelt illustreres slikt:



[85] Den engelske og svenske språkversjonen benytter seg av «indre markedet», mens den danske bruker den tilsynelatende mer vidtfavnende ordlyden «omsætning i Unionen».
[86] KI-forordningen fortalepunkt 1 og artikkel 1 (1) og 2 (1).
[87] KI-forordningen fortalepunkt 26.
[88] KI-forordningen artikkel 3 (2).
[89] KI-forordningen artikkel 5.
[90] KI-forordningen artikkel 6.
[91] KI-forordningen artikkel 50.
[92] KI-forordningen artikkel 51.
[93] Men pålegges noen generelle plikter, se KI-forordningen artikkel 4.

Denne risikobaserte tilnærmingen til kategoriseringen av KI-systemer har likheter med den risikobaserte tilnærmingen en har til vurderingen av hva som er egnede tekniske og organisatoriske tiltak etter GDPR artikkel 32 (1) og (2) – en tilnærming som gjennomsyrer GDPR for øvrig.[94] Vurderingen av hvilke tiltak som er egnede, og som den behandlingsansvarlige og databehandlerne dermed må gjennomføre ved behandlingen av personopplysninger, skal blant annet hensynta «risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter» som behandlingen utgjør.[95]

Denne risikobaserte tilnærmingen vil være relevant for den analytiske gjennomgangen av KI-forordningen artikkel 10 (5) og 59 i punkt 4.2 og 4.3, og utgjør i KI-forordningen et lovgivningsteknisk bakgrunnsteppe for vilkårene og utformingen av disse bestemmelsene. Jo større risiko KI-systemet utgjør overfor individers rettigheter og friheter, desto strengere krav vil lovgiver naturligvis stille til det tiltenkte sikkerhetsnivåmålet, og til de tiltakene som må foretas for å benytte seg av det supplerende rettsgrunnlaget.[96]

En annen likhet KI-forordningen har med personvernforordningen, er rollefordelingen i form av bruken av forskjellige aktører internt i forordningen. Denne rollefordelingen sørger for at regelverket blir håndhevd i praksis. Dette gjøres ved å plassere plikter hos de forskjellige aktuelle aktørene, og for å sørge for at ansvaret for brudd på disse pliktene i forordningen blir plassert hvor lovgiver har ansett det rettmessig.[97] Dette har lovgivningsteknisk store likhetstrekk med aktørene i GDPR som tidligere nevnt i punkt 2.2. Aktørene i KI-forordningen vil bli redegjort for i punkt 3.3.

I de følgende punktene vil det redegjøres for forbudte og høyrisiko KI-systemer. Det avgrenses mot å redegjøre for andre KI-systemer. Disse systemene vil ikke komme på spissen i oppgaven, og er ikke nødvendige for å forstå grunnoppbyggingen av KI-forordningen, eller de utvalgte bestemmelsene som har krysningspunkt med personvernforordningen. Unntaket er forbudte KI-systemer, som vil gjennomgås for å belyse KI-forordningens risikobaserte kategoriseringssystematikk.

[94] Jarbekk og Sommerfeldt (2024), s. 36-37, og Voigt og von dem Bussche (2024), s. 40–41.
[95] GDPR artikkel 32 (1), dette vil bli redegjort for i kapittel 4.
[96] Dette vil utdypes i punkt 4.1.2.
[97] KI-forordningen fortalepunkt 83–84.

3.2 Forbudte og høyrisiko KI-systemer

3.2.1 Forbudte KI-systemer

KI-systemer som har en uakseptabel risiko, er forbudt, jfr. KI-forordningen artikkel 5. Risikoen til et KI-system anses som uakseptabel høy når den går imot unionens verdier om «respect for human dignity, freedom, equality, democracy and the rule of law and fundamental rights enshrined in the Charter, including the right to non-discrimination, to data protection and to privacy and the rights of the child».[98] Det er altså tale om KI-systemer som går mot kjerneverdier innenfor EU-retten samt EUs charter om grunnleggende rettigheter, og som oppfattes som særlig inngripende overfor borgerne. Listen over forbudte KI-systemer er uttømmende regulert. Eksempler på slike forbudte KI-systemer etter KI-forordningen er:

- KI-systemer som benytter seg av subliminale, manipulerende eller villedende teknikker som forstyrrer en person eller gruppes evne til å ta informerte valg, og dermed tar valg som vil eller kan føre til skade på enkeltpersonen eller gruppen, og som de ellers ikke ville tatt.[99]

- KI-systemer som evaluerer eller klassifiserer enkeltindivider eller grupper basert på sosial atferd eller personlige karakstisikker for å gi dem en atferdsbasert poengsum, dersom dette leder til skadelig eller ugunstig behandling i urelaterte sosiale sammenhenger, eller som er uberettiget eller uforholdsmessig.[100]

- KI-systemer som basert på personlighetstrekk og karakteristikker skal foreta risikovurderinger for å forutsi sannsynlighet for at noen skal begå en forbrytelse.[101]

Dette er KI-systemer som gjør dype inngrep inn i enkeltindividers privatsfære og som kan ha vidtrekkende og graverende konsekvenser for dem det gjelder. KI-forordningen har dermed som mål å forhindre at disse blir benyttet overfor EU-borgere, og straffer brudd på dette forbudet med overtredelsesgebyrer opp til 35 000 000 euro eller 7 % av den samlede globale årlige omsetningen.[102]

[98] KI-forordningen fortalepunkt 28.
[99] KI-forordningen artikkel 5 (1) bokstav a.
[100] KI-forordningen artikkel 5 (1) bokstav c, i og ii.
[101] KI-forordningen artikkel 5 (1) bokstav d.
[102] KI-forordningen artikkel 99 (3).

3.2.2 Høyrisiko KI-systemer

Hvorvidt et KI-system skal anses som høyrisiko beror hovedsakelig på hvorvidt det er inntatt i bilag III av KI-forordningen, jfr. KI-forordningen artikkel 6 (2). Eksempler på høyrisiko KI-systemer som er inntatt i bilag III er KI-systemer som skal bistå juridiske myndigheter i deres arbeid, for eksempel å tolke loven,[103] eller KI-systemer som skal evaluere jobbkandidater under en ansettelsesprosess.[104]

Om et KI-system skal *tilføyes* bilag III av EU-kommisjonen beror på om KI-systemet: 1. skal brukes på et bruksområde nevnt i bilag III, og 2. hvorvidt det utgjør «a risk of harm to health and safety, or an adverse impact on fundamental rights», og faren er *tilsvarende* eller *større* enn risikoen KI-systemene som allerede er inntatt i KI-forordningen utgjør, jfr. KI-forordningen artikkel 7 (1) bokstav a og b.

Videre vil KI-systemer som enten utgjør en sikkerhetskomponent i et produkt eller selv er et produkt, og som er omfattet av EUs harmoniseringslovgivning i bilag I, også anses som høyrisiko dersom det før omsetting eller bruk på det indre markedet kreves en overensstemmelsesvurdering foretatt av en tredjepart etter nevnte harmoniseringslovgivning.[105]

Risikoen ved bruk av høyrisiko KI-systemer er ikke tilsvarende graverende som ved forbudte. Den høye risikoen fordrer likevel vesentlige restriksjoner og reguleringer sammenlignet med andre kategorier av KI-systemer som skal selges eller på annen måte tilgjengeliggjøres på markedet, og som har lavere grad av risiko. KI-forordningen regulerer hovedsakelig høyrisiko KI-systemer og bruken av dem, ettersom dette er KI-systemene som utgjør høyest risiko overfor helse, sikkerhet og fysiske personers grunnleggende rettigheter,[106] men som likevel fortsatt er tillatt å ta i bruk.

Høyrisiko KI-systemer vil likevel trolig utgjøre fåtallet av KI-systemer. I en «impact assessment» gjort av EU-kommisjonen i april 2021 ble bare 5–15 % av KI-systemer i Europa antatt kategorisert som høyrisiko.[107] At et KI-system klassifiseres som høyrisiko, og ikke

[103] KI-forordningen Bilag III (8) bokstav a.
[104] KI-forordningen Bilag III (4) bokstav a.
[105] KI-forordningen artikkel 6 (1) bokstav a og b.
[106] KI-forordningen fortalepunkt 1 og 46 siste setning, og artikkel 1.
[107] Europakommisjonen – Impact Assessment, s. 68.

forbudt, betyr ikke nødvendigvis at KI-systemet er *lovlig*. Både andre rettsakter fra EU og EU-kompatibel nasjonal rett kan gjøre bruken av et særskilt KI-system ulovlig.[108]

3.3 Aktører

3.3.1 Provider

Lignende med GDPR benytter KI-forordningen også aktører. En av dem er «provider», og som er enhver:

> *[…] natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge*.[109]

En «provider», også kalt «udbyder» eller «leverantör» i henholdsvis den danske og svenske språkversjonen, defineres dermed hovedsakelig ut ifra hvorvidt de utvikler eller tilgjengeliggjør et KI-system. Mens det ikke foreligger en offisiell norsk oversettelse, er betegnelsen «leverandør» hyppig brukt på norsk, blant annet av Digitaliseringsdirektoratet.[110] Denne betegnelsen vil bli lagt til grunn heretter.

Leverandører av KI-systemer er pålagt en rekke forpliktelser etter KI-forordningen, og er sammen med «deployers» pålagt av KI-forordningen «[p]redictable, proportionate and clear obligations» for å forsikre gjennom hele livssyklusen til KI-systemene trygghet og respekt for eksisterende lovgivning som beskytter enkeltindividers grunnleggende rettigheter.[111]

[108] KI-forordningen fortalepunkt 63.
[109] KI-forordningen artikkel 3 (3).
[110] Eksempelvis i DFØ-rapport 2024:9.
[111] Europakommisjonen – Explanatory Memorandum, punkt 1.1.

3.3.2 Deployer

Med «deployer» menes enhver «natural or legal person, public authority, agency or other body using an AI system under its authority» – med mindre systemet brukes til personlig ikke-ervervsmessig bruk.[112] En «deployer» er dermed en som *bruker* et KI-system, og ble i EU-kommisjonens opprinnelige forslag definert som nettopp «user».[113] Til forskjell fra andre produktsikkerhetsreguleringer pålegger KI-forordningen også en rekke plikter for dem som bruker et KI-system, og ikke bare for dem som utvikler og tilgjengeliggjør det. Disse pliktene innebærer blant annet å sørge for menneskelig tilsyn,[114] å ta egnede tekniske og organisatoriske tiltak for å sørge at en følger de tilhørende instruksene,[115] loggføring,[116] informere berørte ansatte om bruken av høyrisiko KI,[117] foreta en personvernkonsekvensutredning,[118] m.m.

Lignende med at en databehandler kan overta rollen som behandlingsansvarlig etter GDPR,[119] kan en «deployer» overta rollen som leverandør av høyrisiko KI-systemer, og pålegges leverandørens plikter etter KI-forordningen artikkel 16. Dette vil skje dersom de setter sitt eget navn eller varemerke på et høyrisiko KI-system,[120] vesentlig forandrer KI-systemet etter plassering på markedet eller bruk – samtidig med at det forblir et høyrisiko KI-system –[121] eller forandrer de tiltenkte formålene med et ikke-høyrisiko KI-system slik at det faller inn under definisjonen av et høyrisiko KI-system.[122]

Dersom dette skjer, vil den forrige leverandøren ikke lenger anses å være leverandør for dét spesifikke KI-systemet.[123] Dette sørger for at en heller ikke etter KI-forordningen har adgang til å avtale seg vekk fra de forskjellige forpliktelsene, og dermed definere rollene som «provider» og «deployer» på en pliktunnvikende måte seg imellom.

[112] KI-forordningen artikkel 3 (4).
[113] Europakommisjonen – Forslag til KI-forordningen artikkel 3 (4).
[114] KI-forordningen artikkel 26 (2).
[115] Ibid. (1).
[116] Ibid. (6).
[117] Ibid. (7).
[118] Ibid. (9); Se punkt 4.2.7 for mer om personkonsekvensutredninger.
[119] Se punkt 2.2.2 for databehandlerens overtakelse av rollen som behandlingsansvarlig ved instruksbrudd.
[120] KI-forordningen artikkel 25 (1) bokstav a.
[121] Ibid. bokstav b.
[122] Ibid. bokstav c.
[123] Ibid. (2).

4 Krysningspunktet – GDPR og KI-forordningen

4.1 Behandling av personopplysninger

4.1.1 Behandlingsgrunnlag – utgangspunktet

Før KI-forordningen artikkel 10 (5) og 59 gjennomgås, er det nødvendig å forstå det personvernrettslige utgangspunktet for behandling av personopplysninger. Som redegjort for i punkt 2, må den behandlingsansvarlige ha et behandlingsgrunnlag for å behandle personopplysninger. Etter GDPR artikkel 6 foreligger det seks tilfeller hvor den behandlingsansvarlige har et gyldig behandlingsgrunnlag. De seks tilfellene hvor det foreligger et gyldig behandlingsgrunnlag er ved samtykke fra den registrerte,[124] dersom behandlingen er nødvendig for å oppfylle en avtale den registrerte er en part i,[125] nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige,[126] nødvendig for å verne noens vitale interesser,[127] nødvendig for å utføre en oppgave i allmennhetens interesse eller for å utøve offentlig myndighet,[128] eller nødvendig for å forfølge den behandlingsansvarliges berettigede interesser.[129] Foreligger ikke et av disse behandlingsgrunnlagene, er behandlingen ulovlig.[130]

Det er den behandlingsansvarlige som må påvise og er ansvarlig for at det foreligger et slikt behandlingsgrunnlag for behandling av personopplysninger.[131] Terskelen for hva som utgjør en behandling er *lav*. GDPR definerer en behandling som «[…] enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke».[132] Bruk av personopplysninger i et KI-system vil følgelig falle innunder definisjonen.

[124] GDPR artikkel 6 (1) bokstav a.
[125] Ibid. bokstav b.
[126] Ibid. bokstav c.
[127] Ibid. bokstav d.
[128] Ibid. bokstav e.
[129] Ibid. bokstav f.
[130] Ibid. (1).
[131] Ibid. (2).
[132] GDPR artikkel 4 (2).

4.1.2 Behandling av særlige kategorier av personopplysninger

Ønsker man å behandle *særlige kategorier*[133] av personopplysninger, trenger man et rettsgrunnlag i tillegg til et behandlingsgrunnlag etter GDPR artikkel 6.[134] Dette må hjemles i personvernforordningen artikkel 9 (2), og slike særlige kategorier er som tidligere nevnt i punkt 1.3.2 i utgangspunktet forbudt å behandle. Det er altså tale om et unntak fra et forbud. Personvernforordningen artikkel 9 (2) inneholder ti ulike unntak for behandling av særlige kategorier av personopplysninger, hvor den mest aktuelle er uttrykkelig samtykke fra den registrerte for behandling av personopplysninger.[135] For redegjørelsen av KI-forordningen artikkel 10 (5) og artikkel 59 i henholdsvis punkt 4.2 og 4.3, og oppgaven for øvrig, avgrenses redegjørelsen av GDPR artikkel 9 (2) til rettsgrunnlaget i bokstav g.

Slik det fremkommer av KI-forordningens fortale, er KI-forordningen artikkel 10 (5) og 59 tiltenkt å tjene som unionsrettslig hjemmel for et rettsgrunnlag for behandling av særlige kategorier av personopplysninger etter GDPR artikkel 9 (2) bokstav g.[136] GDPR artikkel 9 (2) bokstav g setter opp som vilkår at behandlingen må være: «nødvendig av hensyn til viktige allmenne interesser», hjemlet i «unionsretten» – *et supplerende rettsgrunnlag* – som er forenelig med «det grunnleggende innholdet i retten til vern av personopplysninger», og som «sikre[r] egnede og særlige tiltak» for å «verne den registrertes grunnleggende rettigheter og interesser». Det er altså tale om strenge krav med en høy terskel. At det krever såpass mye for å oppfylle vilkårene for å benytte seg av rettsgrunnlaget, reflekterer alvorligheten assosiert med behandlingen av særlige kategorier av personopplysninger, og at det skal en del til før den behandlingsansvarlige har et unntak til å behandle disse til tross for forbudet.

At lovhjemmelen må «sikre egnede og særlige tiltak» for å «verne den registrertes grunnleggende rettigheter og interesser», pålegger lovgiver etter ordlyden en plikt til å sørge for at det supplerende rettsgrunnlaget lever opp til en viss standard. Den stiller også krav til rettsgrunnlagets kvalitative innhold. At hjemmelen skal sikre «særlige tiltak», vil etter ordlyden innebære at den må gi mer informasjon om og konkretisere hvilke tiltak som skal til for å «verne den registrertes grunnleggende rettigheter og interesser». Dette innebærer videre at rettsgrunnlaget tilføyer nye krav til tiltak for behandlingen *utover* det som allerede følger av

[133] Se punkt 1.3.2 for definisjonen av særlige kategorier.
[134] Skullerud mfl. (2023), Artikkel 9. Behandling av særlige kategorier av personopplysninger, Juridika [Tilgjengelig: https://juridika.no/no/lov/2016-04-27-679/%C2%A79/kommentar/] (lest 22.10.2024).
[135] GDPR artikkel 9 (2) bokstav a.
[136] Se henholdsvis KI-forordningen fortalepunkt 70 og 140.

GDPR. Disse nye tiltakene må være mer tilpasset typesituasjonen enn de mer generelle tiltakene som pålegges behandlingsansvarlige og databehandlere av personvernforordningen. De generelle kravene til behandlingen etter GDPR vil nemlig gjelde uansett,[137] og bestemmelsen hadde vært overflødig hvis den ikke tilføyde noe nytt.

Det er dermed en forutsetning at KI-forordningen artikkel 10 (5) og 59 oppstiller tiltak som da faktisk *er* mer egnet – tilpasset – situasjonen og er mer kasuistisk utformet enn det det som alt foreligger av påkrevde tiltak. Er ikke dette tilfellet, så lever ikke de supplerende rettsgrunnlagene opp til hjemmelskravet. Dette vil i det følgende være i fokus ved analysen av KI-forordningen artikkel 10 (5) og 59, ettersom etterlevelse av hjemmelskravet er en vektig side i analysen av KI-forordningens overordnede samsvar med GDPR.

4.2 KI-forordningen artikkel 10 (5)

4.2.1 Innledning

Som tidligere nevnt, er utgangspunktet etter KI-forordningen artikkel 2 (7) at reguleringen ikke skal «affect Regulation (EU) 2016/679». KI-forordningen gjør det klart at den ikke er ment å påvirke anvendelsen av GDPR. Det følger imidlertid av samme setning at dette utgangspunktet skal legges til grunn «without prejudice to Article 10(5) and Article 59 of this Regulation». Førstnevnte – KI-forordningen artikkel 10 – tar for seg bruken av høyrisiko KI-systemer, og *hvordan* disse skal trenes på data. Bestemmelsen setter en rekke kvalitetskrav som må etterleves for at treningen av et høyrisiko KI-system skal anses lovlig etter KI-forordningen.

Et av disse kvalitetskravene fastsettes etter artikkel 10 (5). Dersom det er «strictly necessary» for å sikre «bias detection and correction» i høyrisiko KI-systemer, kan leverandører av slike systemer «exceptionally» behandle særlige kategorier av personopplysninger,[138] såfremt dette skjer med nødvendige garantier for fysiske personers grunnleggende rettigheter og friheter. Dette er et supplerende rettsgrunnlag som åpner opp for behandling av særlige kategorier av personopplysninger, hjemlet i GDPR artikkel 9 (2) bokstav g, og som nevnt kun er aktuell dersom det skjer «på grunnlag av unionsretten […]». At KI-forordningen her er tiltenkt å

[137] Foruten GDPRs lovsystematikk, følger dette også av KI-forordningen fortalepunkt 140.
[138] For mer om særlige kategorier av personopplysninger, se punkt 1.3.2.

utgjøre et supplerende rettsgrunnlag for behandling av særlige kategorier av personopplysninger etter GDPR artikkel 9 (2) bokstav g, fremkommer direkte av fortalen.[139]

Formålet med Artikkel 10 (5) er å motkjempe diskriminering som følger av «bias» – skjevheter – i høyrisiko KI-systemer.[140] KI-forordningen definerer ikke begrepet «bias», men ordlyden kan tilsi at det er tale om en underliggende forutinntatt mening, fordel eller ulempe som negativt eller positivt kan påvirke enkeltindivider eller grupper på urettferdig vis.[141] Slike «bias» oppstår typisk på grunn av mangler og svakheter med datasettene brukt under opptreningsfasen.[142] Et eksempel er en banks KI-system som uproporsjonalt og utilsiktet avslår visse etnisiteters søk om lån, ettersom den assosierer enkelte postkoder – hvor etnisiteten har en høy konsentrasjon – med dårlig tilbakebetalingsevne.[143] Bestemmelsen understøtter dermed diskrimineringsvernet ved å åpne opp for bruk av særlige kategorier av personopplysninger for å oppdage og korrigere disse «bias[ene]».[144] Det avgrenses mot en ytterligere redegjørelse av diskrimineringsvernsaspektet, ettersom oppgavens fokus er rettsgrunnlagets harmonisering med GDPR. Formålet er imidlertid viktig å ha i mente ettersom artikkel 10 (5) på mange måter er et resultat av EU-lovgivers avveining mellom diskrimineringsvernet og personvernet.

Det er verdt å merke seg at KI-forordningen artikkel 10 (5) ikke utelukker at en behandler særlige kategorier av personopplysninger for tilsvarende formål, men da med et annet rettsgrunnlag etter GDPR artikkel 9 (2). KI-forordningen Artikkel 10 (5) åpner imidlertid opp for at leverandøren i rollen som behandlingsansvarlig nettopp slipper å benytte seg av andre unntak fra forbudet, eksempelvis å måtte innhente et uttrykkelig samtykke fra den registrerte. Dette vil gjøre det lettere for leverandørene å finne et rettsgrunnlag for behandlingen for å sikre «bias detection and correction».

Det er imidlertid viktig å understreke at leverandøren fortsatt trenger et behandlingsgrunnlag for å behandle personopplysningene etter GDPR artikkel 6.[145] Et aktuelt behandlingsgrunnlag er GDPR artikkel 6 (1) bokstav c, som gir behandlingsgrunnlag der behandling av personopplysninger er nødvendig for å oppfylle en rettslig forpliktelse.[146] Etter KI-forordningen

[139] KI-forordningen fortalepunkt 70.
[140] Ibid.
[141] Tolkningen er inspirert av Bekkum (2024), s. 8–9.
[142] Ibid. s. 9.
[143] Eksemplet er inspirert av Bekkum (2024), s. 3–4.
[144] Som fremhevet i Bekkum (2024), s. 8.
[145] Se punkt 4.1.1 for behandlingsgrunnlagene.
[146] Ibid.

artikkel 10 (2) har lovgiver nemlig fastsatt at «[t]raining, validation and testing data sets *shall* be subject to data governance and management practices appropriate for the intended purpose of the high-risk AI system».[147] Disse praksisene skal etter artikkel 10 (2) bokstav f og g henholdsvis bl.a. være «examination in view of possible biases» med negative innvirkninger og «appropriate measures to detect, prevent and mitigate possible biases identified according to point (f)». Dette understøttes av at det supplerende rettsgrunnlaget i artikkel 10 (5) nettopp er myntet på tilfellene hvor «it is strictly necessary for the purpose of ensuring bias detection and correction […] *in accordance with paragraph (2), points (f) and (g)*».[148] Det foreligger dermed en *rettslig forpliktelse* på leverandøren etter artikkel 10 (2).

KI-forordningen fastsetter videre i artikkel 10 (5) at leverandøren må oppfylle en rekke særskilte vilkår for å kunne benytte seg av artikkel 10 (5) som et supplerende rettsgrunnlag, *i tillegg til* å etterleve kravene etter GDPR. Betydningen av at bestemmelsen utskiller disse som tilleggsvilkår vil bli kommentert avslutningsvis i punkt 4.2.8, men er viktig å ha i mente i den følgende analysen av tiltakene i punkt 4.2.2–4.2.7.

4.2.2 Nødvendig

Det første vilkåret etter KI-forordningen artikkel 10 (5) bokstav a er at «bias detection and correction» ikke kan «effectively [be] fulfilled by processing other data, including synthetic or anonymised data». Bestemmelsen setter opp et vilkår om nødvendighet. Kan syntetisk og anonymisert data effektivt oppdage og korrigere skjevheter, er ikke bruken av særlige kategorier av personopplysninger nødvendig.

Tiltaket fremstår imidlertid som overflødig. At en ikke skal behandle flere – eller mer sensitive –[149] personopplysninger enn hva som er nødvendig, følger allerede av et av personvernforordningens grunnprinsipper. Nemlig grunnprinsippet om at personopplysningene en behandler skal være «begrenset til det som er nødvendig for formålene de behandles for», bedre kjent som dataminimeringsprinsippet, jfr. GDPR artikkel 5 (1) bokstav c.[150] Dette legges til grunn i GDPR fortalepunkt 39, ved at «[p]ersonopplysninger bør [bare] behandles […]

[147] Min kursivering.
[148] Min kursivering.
[149] Se Kuner mfl. (2020), s. 317, dataminimeringsprinsippet omfatter ikke bare personopplysnings*kvantitet*, men også *kvalitet*.
[150] Se også GDPR fortalepunkt 39.

dersom formålet med behandlingen ikke med rimelighet kan oppfylles på annen måte». I dette ligger det en implisitt nødvendighetsvurdering for å være i samsvar med prinsippet.[151]

Den behandlingsansvarlige må begrense seg til å behandle de personopplysningene som er nødvendige for å oppnå formålene med behandlingen. Alternativt – dersom det ikke er nødvendig – ikke behandle *noen* personopplysninger.[152] Å utskille dette som et eget selvstendig tilleggsvilkår, som skal hensyntas utover det som følger av GDPR, utgjør dermed ikke et særlig tiltak.

4.2.3 Sikkerhets- og privatlivsbeskyttende tiltak

KI-forordningen artikkel 10 (5) bokstav b fastsetter at de særlige kategoriene av personopplysninger skal være underlagt «technical limitations on the re-use of the personal data» samt «state-of-the-art security and privacy-preserving measures», herunder pseudonymisering.[153]

Lignende, etter GDPR artikkel 32 (1), skal den behandlingsansvarlige og databehandleren «gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen» idet det hensyntas «den tekniske utviklingen».

Den brede ordlyden «egnede tekniske og organisatoriske tiltak» hensyntatt «den tekniske utviklingen» (EN: «state of the art») i GDPR artikkel 32 (1) fanger allerede i utgangspunktet opp KI-forordningens artikkel 10 (5) bokstav b «state-of-the-art security and privacy-preserving measures». Mens KI-forordningen oppsetter disse vilkårene «statisk» – det vil si, uten å relativisere det ut fra risikoen – har GDPR en risikobasert tilnærming. Det innebærer at jo større risiko, desto strengere tiltak krever de dynamiske kravene etter GDPR for å oppnå en tilfredsstillende høy grad av sikkerhets- og privatlivsbeskyttende tiltak. Altså et «egnet» nivå. Etter GDPR er det klart at det er den behandlingsansvarlige og databehandleren som selv må finne de tiltakene som er passende for risikoen.[154]

Som EU-domstolen har påpekt i *VB [C5]* C-340/21 på avsnitt 42, må man foreta en todelt vurdering for å finne ut om et tiltak er egnet. Det er først nødvendig å «[…] identify the risks

[151] Skullerud mfl. (2023), Artikkel 5. Prinsipper for behandling av personopplysninger, Juridika [Tilgjengelig: https://juridika.no/no/lov/2016-04-27-679/%C2%A75/kommentar/] (lest 14.10.2024).
[152] EDPB – Retningslinje 04/2019, avsnitt 76.
[153] Se GDPR artikkel 4 (5) for definisjonen av pseudonymisering.
[154] Kuner mfl. (2020), s. 635.

of a personal data breach caused by the processing concerned and their possible consequences for the rights and freedoms of natural persons», for å så «[…] ascertain whether the measures implemented by the controller are appropriate to those risks, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of that processing».

Særlige kategorier av personopplysninger vil av sin sensitive art kreve en høyere grad av beskyttelse,[155] og da særlig i konteksten trening av høyrisiko KI-systemer. Slike KI-systemer utgjør i utgangspunktet og per definisjon nettopp en stor risiko for individers fundamentale rettigheter.[156] Det vil dermed stilles strenge krav etter personvernforordningen før et sikkerhets- og privatlivsbeskyttende tiltak etter GDPR artikkel 32 (1) i en KI-forordning-artikkel 10 (5)-situasjon kan anses som «egnet».

Mens KI-forordningen ikke sier *hva* standarden er, henviser den som nevnt likevel til hva som er «state-of-the-art» innenfor sikkerhets- og privatlivsbeskyttende tiltak. Dette fremstår intetsigende og gir lite veiledning. Hva som til enhver tid er det absolutte «state-of-the-art» av tiltak, vil variere og være vanskelig å stadfeste. Ordlyden oppsetter dermed et absolutt, men et innholdsmessig ukjent krav.

Tilsvarende skal hva som er «state of the art» som nevnt hensyntas etter GDPR artikkel 32 (1) ved iverksetting av tiltak. Her spesifiseres det imidlertid at sikkerhetsnivået som oppnås ved dette skal være «egnet». Dette gir den behandlingsansvarlige og databehandlere et spillerom for hvilke tiltak som skal iverksettes.[157] Som EDPB har påpekt, er begrepet etter GDPR «[…] a dynamic concept that cannot be statically defined at a fixed point in time, but should be assessed *continuously* in the context of technological progress.»[158] Artikkel 32 (1) setter videre krav til tiltak, ikke resultat.[159] Dette har blitt stadfestet av EU-domstolen blant annet i *MediaMarktSaturn [C5]* C-687/21 avsnitt 39, nemlig at «[…] the controller is obliged to mitigate the risks of personal data breaches and not prevent all breaches of those data».

[155] Skullerud mfl. (2023), Artikkel 32. Sikkerhet ved behandlingen, Juridika [Tilgjengelig: https://juridika.no/no/lov/2016-04-27-679/%C2%A732/kommentar/] (lest 06.09.2024).
[156] Se KI-forordningen fortalepunkt 48.
[157] Voigt og von dem Bussche (2024), s. 40–41.
[158] EDPB – Retningslinje 04/2019, avsnitt 20, riktig da som en kommentar angående GDPR artikkel 25 (1), men ordlyden er tilsvarende.
[159] Kuner mfl. (2020), s. 637.

At KI-forordningen i kontrast oppstiller dette som et absolutt vilkår, vil på grunn av dens innholdsmessige flytende natur bli tilnærmet umulig å etterleve. Det overnevnte utsagnet fra EDPB angående «state of the art» illustrerer hvor høye krav det isolert sett stilles for å etterleve hva som er «state-of-the-art» etter KI-forordningen. Dette står i motsetning til kravet etter GDPR artikkel 32 (1), som kun er mulig å etterleve i en GDPR-kontekst ettersom «state of the art»-kravet der kun skal hensyntas som ett av flere moment i en større dynamisk og sammensatt egnethetsvurdering. De strenge kravene til sikkerhets- og privatlivsbeskyttende tiltak i KI-forordningen vil i praksis trolig tvinge leverandørene til å falle tilbake på hva de løpende anser som egnet ut fra den høye risikoen, framfor å finne ut hva som objektivt sett er «state-of-the-art».

Bestemmelsen fremstår altså ikke som særlig tilpasset eller tydelig på hvilke tiltak som skal iverksettes.[160] De generelle og dynamiske kravene etter GDPR vil langt på vei stille tilsvarende strenge krav til hvilke sikkerhets- og privatlivsbeskyttende tiltak den behandlingsansvarlige må gjennomføre, men vil i motsetning være enklere å etterleve. Videre er pseudonymisering allerede særskilt nevnt som et tiltak som – dersom egnet – skal tas for å sikre «egnede tekniske og organisatoriske tiltak», jfr. GDPR artikkel 32 (1) bokstav a. Det er altså vanskelig å se hvordan forordningene i realiteten ikke er fullstendig overlappende på dette punktet, og hvordan KI-forordningen artikkel 10 (5) bokstav b gir et bidrag til sikkerheten av personopplysningene utover det som allerede følger av GDPR, foruten å skape større usikkerhet over hvilke tiltak som er tilstrekkelige.

4.2.4 Konfidensialitet

Videre skal de særlige kategoriene av personopplysninger etter KI-forordningen artikkel 10 (5) bokstav c være «subject to measures» som skal forsikre at personopplysningene som blir behandlet er «secured», «protected», og «subject to suitable safeguards» herunder sistnevnte «including strict controls and documentation of the access». Dette er for å sørge for at *kun* personer med «appropriate confidentiality obligations» har adgang.

[160] Som GDPR artikkel 9 (2) bokstav g krever av det supplerende rettsgrunnlaget, se punkt 4.1.2.

«[M]easures» som skal sikre at personopplysningene er «secured», «protected» og «subject to suitable safeguards», er allerede omfattet av ordlyden «egnede tekniske og organisatoriske tiltak» etter GDPR artikkel 32 (1).[161] Tekniske og organisoriske tiltak som ikke tilfredsstiller disse vilkårene, kan etter den brede ordlyden vanskelig anses som «egnet».

Hva angår adgang til personopplysningene og konfidensialitet, er dette allerede omfattet eksplisitt i GDPR artikkel 32 (1) bokstav b, se «sikre vedvarende konfidensialitet», og GDPR artikkel 32 (2), se hensynet som skal tas ved risikovurderingen for utilsiktet «ikke-autorisert utlevering av eller tilgang til personopplysninger». Tilsvarende uttrykkes gjennom GDPR artikkel 32 (4), ved at den behandlingsansvarlige og databehandleren skal forsikre seg om at fysiske personer med tilgang til personopplysningene «behandler […] [person]opplysninger bare etter instruks fra den behandlingsansvarlige».

Videre er prinsippet om integritet og konfidensialitet et av de grunnleggende prinsippene som gjennomsyrer og begrunner de forskjellige lovregulerte forpliktelsene som pålegges etter GDPR. Dette utrykkes utvetydelig i GDPR artikkel 5 (1) bokstav f. Brudd på de grunnleggende prinsippene i GDPR artikkel 5 (1) bokstav a-f er i seg selv et brudd etter forordningen, se GDPR artikkel 5 (2). De høyeste overtredelsesgebyrene etter GDPR gis nettopp ved brudd av de grunnleggende prinsippene for behandling, jfr. GDPR artikkel 83 (5) bokstav a. Både GDPR artikkel 32 og de mer vidtgående grunnprinsippene dekker dermed tiltakene, og gjør KI-forordningen artikkel 10 (5) bokstav c overflødig.

4.2.5 Ikke blir oversendt

De særlige kategoriene av personopplysninger som blir behandlet skal videre ikke bli «transmitted, transferred or otherwise accessed» av «other parties», jfr. KI-forordningen artikkel 10 (5) bokstav d. Denne bestemmelsen utrykkes «relativt» i flere av de overnevnte bestemmelsene fra GDPR, da særlig konfidensialitet og utilsiktet tilgang. GDPR oppsetter imidlertid ikke noen harde forbud mot å videresende særlige kategorier av personopplysninger til tredjeparter.

Mens kravene til konfidensialitet *kan* – for å være «egnet» –[162] kreve at informasjonen ikke under noen omstendigheter skal oversendes til andre parter, er imidlertid dette sjeldent aktuelt,

[161] For mer om artikkel 32 (1), se punkt 4.2.3.
[162] Se GDPR artikkel 32 (1) bokstav b og punkt 4.2.4.

og kan ikke oppstilles som et absolutt krav ved all bruk av KI etter GDPR. Personvernforordningen har ikke noe utgangspunkt om at særlige kategorier aldri kan deles til tredjeparter. Den vil imidlertid kreve flere og bedre tekniske og organisatoriske tiltak for å ivareta sikkerheten og bøte på risikoen assosiert med å oversende særlige kategorier av personopplysninger, kontra alminnelige personopplysninger. Dersom dette, samt et rettsgrunnlag etter GDPR artikkel 9 (2) foreligger, er oversending, overføring og annen tilgjengeliggjøring generelt tillatt og i samsvar med GDPR.

Videre, og betydelig mer problematisk, er det usikkert om KI-forordningen med delingsforbudet har ment å forby bruken av databehandlere, ettersom disse etter ordlyden vil omfattes av «other parties».[163] I GDPR er «tredjepart[er]» (engelsk: «third party») legaldefinert som enhver annen *enn* databehandlere, m.m.[164] Begrepet ble tilsvarende definert i det tidligere personverndirektivet.[165] Dersom KI-forordningens ordlyd *ikke* er ment å ekskludere databehandlere, er det vanskelig å se hvorfor lovgiver har valgt en annen terminologi enn den som allerede er godt etablert – og legaldefinert – på personvernrettsfeltet. Å henvise til – og benytte seg av – andre og etablerte legaldefinisjoner i andre forordninger/direktiver er videre en lovgivningsteknikk som hyppig brukes av EU for å nettopp sikre uniform forståelse og anvendelse av de samme konseptene på tvers av rettsaktene. Se f.eks. legaldefinisjonen av særlige kategorier av personopplysninger og personopplysninger i henholdsvis KI-forordningen artikkel 3 (37) og (50). En kontekstuell tolkning tilsier heller ikke at databehandlere er ment å være unntatt fra KI-forordningens generelle forbud mot deling med «other parties».

Dette vil da utelukke at noen behandler særlige kategorier av personopplysninger på leverandørens vegne for å bidra med å motkjempe og korrigere skjevheter i KI-systemene. Dette vil i så fall være svært uheldig. Databehandlere som over tid bygger opp inngående kompetanse i å effektivt motkjempe skjevheter i KI-systemer, kan da ikke tilby sine tjenester til utviklere av KI-systemer. Leverandørene vil da bli tvunget til å løse dette på egenhånd. Databehandlertjenester utgjør på generelt grunnlag dessuten ofte sentrale funksjoner i

[163] Det er viktig å merke seg at bestemmelsen er myntet på leverandøren, som i denne situasjonen *ikke* kan være en databehandler. Det er fordi bestemmelsen kun gir et supplerende rettsgrunnlag til *leverandøren*. Etter GDPR er det bare behandlingsansvarlige som kan inneha slike rettsgrunnlag. Databehandlere kan kun *utlede* dette gjennom en databehandleravtale med en behandlingsansvarlig. Leverandøren *må* altså i artikkel 10 (5)-situasjoner være behandlingsansvarlig. At databehandleren skal kunne behandle personopplysninger, men ikke den behandlingsansvarlige, gir ikke mening. Se for øvrig punkt 2.2.
[164] Se GDPR artikkel 4 (10).
[165] Se Direktiv 95/46/EF artikkel 2 bokstav f.

behandlingen av personopplysninger, for eksempel lagringstjenester.[166] Den behandlingsansvarlige vil da fort ende med å bryte med KI-forordningen dersom den benytter seg av disse tredjemannstjenestene. Å kategorisk utelukke disse ved skjevhetskorrigering og -oppdagelse av KI-systemer er lite hensiktsmessig, og vil trolig gjøre det uforholdsmessig vanskelig for leverandører å luke ut skjevheter fra sine systemer.

Det fremstår påfallende at KI-forordningen skal stenge for en såpass sentral del av databehandlingssfæren som databehandlere utgjør uten å drøfte problemstillingen i fortalen eller under lovgivningsprosessen. Både bestemmelsens ordlyd, valget av ordlyden «in addition» i KI-forordningen artikkel 10 (5), samt ordlyden «without prejudice» i KI-forordningen artikkel 2 (7), åpner derimot for at KI-forordningen nettopp kan avvike løsningen etter GDPR og særregulere disse tilfellene. KI-forordningen artikkel 10 (5) bokstav d fremstår som lite gjennomtenkt, og som en dårligere løsning enn det som allerede følger av GDPR.

4.2.6 Sletting av personopplysninger

At personopplysningene skal slettes «once the bias has been corrected», jfr. KI-forordningen artikkel 10 (5) bokstav e, kan utledes allerede fra grunnprinsippene i GDPR: personopplysninger skal ikke lagres «i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for», jfr. GDPR artikkel 5 (1) bokstav e. Det samme følger av GDPR artikkel 17 (1) bokstav a: den registrerte har rett til å få sine personopplysninger slettet dersom personopplysninger ikke lenger er «nødvendige for formålet som de ble samlet inn eller behandlet for». Er skjevheten korrigert, er formålet for behandlingen av personopplysningene oppnådd.

Videre skal personopplysningene etter KI-forordningen slettes når de har nådd «the end of its retention period». Denne plikten følger og defineres allerede av lagringsbegrensningsprinsippet etter overnevnte GDPR artikkel 5 (1) bokstav e.

Det er imidlertid interessant at KI-forordningen her ikke tar stilling til slettingsplikten og dens betydning for *oppdagelse* av skjevheter. Det vil være vanskelig for en leverandør å vite om alle skjevheter i et KI-system faktisk *er* oppdaget og korrigert. Dette gjør at det kan være uheldig for leverandører å korrigere skjevheter løpende, og at en heller venter til at eventuelle skjevheter

[166] Datatilsynet – «Hva er en databehandler?»

har samlet seg opp. Dette er fordi de særlige kategoriene av personopplysninger etter ordlyden må slettes «*once* the bias has been corrected».[167] De må dermed slettes allerede ved første skjevhetskorrigering, og kan som en konsekvens ikke benyttes til å finne andre potensielle uoppdagede skjevheter – eksisterende eller fremtidige. Mens dette trolig ikke har vært lovgivers intensjon,[168] så gir den uklare ordlyden et uheldig tolkningsrom.

4.2.7 Begrunnelse i behandlingsprotokollene

Det siste vilkåret etter KI-forordningen artikkel 10 (5) bokstav f er at behandlingsprotokollene etter GDPR artikkel 30 inkluderer begrunnelsen for *hvorfor* det var strengt nødvendig å behandle særlige kategorier av personopplysninger for å oppdage og korrigere skjevheter, og hvorfor dette formålet ikke kunne nås ved bruk av andre data. Dette er nytt ved KI-forordningen og har ikke en direkte tilsvarende regulering etter GDPR. Et krav om å rettferdiggjøre behandlingen i behandlingsprotokolen foreligger ikke etter GDPR artikkel 30 eller GDPR for øvrig.

Personvernforordningen krever at en behandlingsansvarlig som planlegger å foreta behandlingsaktiviteter som «medføre[r] en høy risiko for fysiske personers rettigheter og friheter», skal foreta en vurdering av personvernkonsekvensene, jfr. GDPR artikkel 35 (1). Slike vurderinger kalles en «Data Protection Impact Assessment» på engelsk, ofte forkortet «DPIA». En DPIA skal minst inneholde «en vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene», jfr. GDPR artikkel 35 (7) bokstav b. Det ligger i høyrisiko KIs natur at de utgjør en «høy risiko for fysiske personers rettigheter og friheter».[169] At en behandler sensitive personopplysninger, herunder særlige kategorier av personopplysninger, er i seg selv et moment i vurderingen av hvorvidt en skal utføre en DPIA.[170] I en slik personvernkonsekvensvurdering er det naturlig å vurdere både hvorvidt en *trenger* å behandle særlige kategorier av personopplysninger, og for hvor lang tid.[171] At en ikke skal behandle flere – eller mer sensitive – personopplysninger enn hva som er nødvendig, følger som tidligere nevnt av dataminimeringsprinsippet, jfr. GDPR artikkel 5 (1) bokstav c.[172]

[167] Min kursivering.
[168] Rettskildene er tause angående problemstillingen.
[169] Se KI-forordningen fortalepunkt 48.
[170] Artikkel 29-gruppen – Retningslinje (2017), s. 9.
[171] Skullerud mfl. (2023), Artikkel 35. Vurdering av personvernkonsekvenser, Juridika [Tilgjengelig: https://juridika.no/no/lov/2016-04-27-679/%C2%A735/kommentar/] (lest 09.09.2024).
[172] Se punkt 4.2.2 for mer om dataminimeringsprinsippet.

Selv om det altså ikke stilles krav om at den behandlingsansvarlige fører nødvendighetsvurderingen inn i behandlingsprotokollene etter GDPR, vil GDPR uansett pålegge den behandlingsansvarlige å foreta en tilsvarende vurdering om behandlingsaktivitetens nødvendighet gjennom DPIA-en. Vurderingene vil da ha store overlapp. KI-forordningen kunne dermed ha unngått unødvendig dobbeltarbeid ved å minimum stadfeste at personvernkonsekvensvurderingen alltid skal foretas, eller ved å bestemme at denne skal inkluderes i behandlingsprotokollene. Å oppstille dette som et nytt selvstendig krav – med tilhørende selvstendig vurdering – fremstår unødvendig.

4.2.8 Refleksjoner samt lovgivningsprosessen bak artikkel 10 (5)

I lys av den overnevnte analysen er det vanskelig å se hvordan kravene etter KI-forordningen artikkel 10 (5) skal forstås med tanke på forholdet til personvernforordningen. Utgangspunktet i KI-forordningen etter artikkel 2 (7) er at KI-forordningen *ikke* skal virke inn på GDPR, men da med *unntak* for KI-forordningen artikkel 10 (5). Etter artikkel 10 (5) følger det derimot at vilkårene etter GDPR *skal følges*, men at det *også* skal legges til grunn noen *tilleggsvilkår* for behandling av særlige kategorier av personopplysninger ved oppdagelse og korrigering av bias.

Som redegjort for ovenfor, ser det imidlertid ikke ut til at det er tale om noen tilleggsvilkår, men at det i stor grad foreligger en dobbelregulering av de forpliktelsene som allerede følger av GDPR og som er pålagt behandlingsansvarlige og databehandlere. Dette harmoniserer dårlig med GDPR artikkel 9 (2) bokstav g, som forutsetter som nevnt i punkt 4.1.2 at det supplerende rettsgrunnlaget for behandling av særlige kategorier av personopplysninger kommer med *nye* tiltak i tillegg til de eksisterende, ikke å dobbeltregulere dem. Denne bestemmelseskjeden med hovedregler, unntak, og tilleggsvilkår fremstår – sammen med artikkel 2 (7) – lite gjennomtenkt og unødvendig.

Tiltakene etter KI-forordningen artikkel 10 (5) fremstår altså hverken mer tilpasset typesituasjonen, eller tydeligere på hvilke tiltak som konkret skal til for å verne om den registrerte, enn det som følger av GDPR. *Hvordan* artikkel 10 (5) kan ha fått denne utformingen, vil utforskes i det følgende.

Dagens ordlyd og EU-kommisjonens forslag

I EU-kommisjonen opprinnelige lovforslag foreligger hverken den uheldige bestemmelsesrekken om forordningens virkeområde,[173] ordlyden «in addition» som oppstiller tilleggsvilkår,[174] eller selve tilleggsvilkårene som dobbeltregulerer og på en ugunstig måte påvirker aktørfordelingen etter GDPR.[175] Særlig ordlyden «in addition» forandrer anvendelsen av regelverket.

I det opprinnelige lovforslaget er ordlyden at behandlingen av særlige kategorier av personopplysninger skal være «subject to appropriate safeguards for the fundamental rights and freedoms of natural persons».[176] For å konkretisere *hvilke* nødvendige garantier som er egnede, benytter lovforslaget seg av ordlyden «including» når den henviser til tiltak som pseudonymisering, «state-of-the-art security and privacy-preserving measures», m.m., fremfor KI-forordningens «in addition». Denne ordlyden eksemplifiserer og plasserer egnethetsvurderingen av hva som er nødvendige garantier naturlig inn under personvernregelverket, fremfor å utskille, sidestille, og absoluttere vilkårene.

Mens disse endringene synes å være resultat av et ønske om å forsterke og fremheve personvernet, virker det imidlertid som om at det ved revideringen av EU-kommisjonens forslag til KI-forordningen artikkel 10 (5) ikke ble tatt i betraktning det eksisterende personvernregelverket med dets tilhørende personvernverktøy, og at samspillet med GDPR som en konsekvens ikke er tilstrekkelig vurdert og problematisert. Personopplysningsvernet har tilsynelatende fått et sent, men særlig fokus etter EU-kommisjonen la frem sitt forslag. Det kan ha ført til at de GDPR-relaterte aspektene ved reguleringen har blitt fremhevet, men ikke tilstrekkelig overveid. Særlig dette vil utforskes nedenfor.

[173] Sammenlign EU-kommisjonens forslag artikkel 2 og KI-forordningen artikkel 2 (7).
[174] Sammenlign EU-kommisjonens forslag artikkel 10 (5) og KI-forordningen artikkel 10 (5).
[175] Sammenlign EU-kommisjonens forslag artikkel 10 (5) og KI-forordningen artikkel 10 (5) bokstav a-f.
[176] Som en henvisning til at begrepet «special categories of personal data» skal forstås tilsvarende som etter GDPR, EUDPR og personverndirektivet for politi og påtalemyndighet.

Artikkel 10 (5) under lovgivningsprosessen

I Rådet for Den europeiske Unions generelle innstilling fra 25.11.2022,[177] er de overnevnte forandringene ikke tatt med. I den endelige kompromissteksten av 26.01.2024, som ble til etter en foreløpig avtale inngått 9.12.2023 etter forhandlinger mellom Europaparlamentet og Rådet for Den europeiske Union, er tilleggsvilkårene tatt med, uten at dette diskuteres videre i forslagets forklarende innledning.[178] Disse tilleggsvilkårene ble tatt med den 14.06.2023 av Europaparlamentet[179] etter et utkast til betenkning fra 22.05.2023 av de ansvarlige parlamentskomiteene.[180] Opprinnelig, etter komiteenes betenkning fra 20.04.2022, ble hele EU-kommisjonens forslag til artikkel 10 (5) foreslått slettet, med den begrunnelse at KI-forordningen «[…] should not constitute a separate legal basis for processing personal data.»[181] Også EDPB uttrykte i en felles uttalelse med Det europeiske datatilsynet bekymring for at artikkel 10 (5) ikke var tydelig nok og trengte ytterligere beskyttelsestiltak dersom bestemmelsen skulle utgjøre et supplerende rettsgrunnlag.[182]

I listen over EU-parlamentarikernes endringsforslag 1581–2005 av 13.06.22 ble det imidlertid foreslått i endringsforslag 1738 til Europaparlamentet å beholde det supplerende rettsgrunnlaget, men med *ytterligere vilkår* for behandling.[183] De fleste andre endringsforslagene ville fjerne artikkel 10 (5).[184] Disse ble vedtatt som Europaparlamentets mandat for interinstitusjonelle forhandlinger den 14.06.2023, da med en annen utforming og ordlyd.[185] Det var med utgangspunkt i disse ekstra tilleggsvilkårene at Parlamentet la frem sitt forslag ved den første trilogforhandlingen av 18.07.2023,[186] og Parlamentet og Rådet ble enige om ordlyden på tilleggsvilkårene etter den andre trilogforhandlingen av 2/3.10.2023.[187] En trilogforhandling er et uformelt møte mellom Europaparlamentet og Rådet for Den europeiske Union, hvor EU-kommisjonen fungerer som megler for å løse politiske uenigheter mellom de

[177] Rådet for Den europeiske union, «Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights», *Rådet for Den europeiske union*, 6. desember 2022 [Tilgjengelig: https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/] (lest 03.09.2024).
[178] Rådet for Den europeiske union – Endelig kompromisstekst, s. 119–120.
[179] Det europeiske parlament – Vedtatte endringer, 14. juni 2023, s. 158–159.
[180] Det europeiske parlament – Betenkning, 22. mai 2023, s. 167–168.
[181] Det europeiske parlament – Utkast til betenkning, 20. april 2022, s. 63.
[182] EDPB og EDPS – Felles uttalelse 05/2021, punkt 3.4.
[183] Det europeiske parlament – Endringsforslag 1581-2005, 13. juni 2022, s. 71–72.
[184] Ibid.
[185] Det europeiske parlament – Vedtatte endringer, 14. juni 2023, s. 158–159.
[186] Interinstitusjonelle forhandlinger – Trilog av 18. juli 2023, s. 278–280.
[187] Interinstitusjonelle forhandlinger – Trilog av 2. og 3. oktober 2023, s. 353–357.

to institusjonene.[188] Det var også i denne andre trilogforhandlingen at ordlyden «including» ble fjernet i favør av «in addition».[189] På grunn av trilogforhandlingenes karakter som uformelle forhandlinger, finnes det ingen dokumenter på hva som ble sagt eller diskutert som kan ha ført til at ordlyden ble endret.

I løpet av lovgivningsprosessen ble tilleggsvilkårene tilføyd KI-forordningen artikkel 10 (5) tilsynelatende på grunn av tvil om EU-kommisjonens opprinnelige lovforslag alene sikret en adekvat og betryggende sikkerhet rundt det supplerende rettsgrunnlaget. Det har derfor vært nødvendig å betrygge de forskjellige aktørene i lovgivningsprosessen om at de personvernrettslige aspektene ville bli særskilt hensyntatt dersom KI-forordningen artikkel 10 (5) skulle utgjøre et supplerende rettsgrunnlag for behandling av særlige kategorier av personopplysninger etter GDPR artikkel 9 (2) bokstav g.

Ordlyden «in addition» ble imidlertid ikke foreslått av en fagkomité, men ble politisk fremforhandlet mellom EU-parlamentet og Rådet med EU-kommisjonen som megler – og da relativt sent i lovgivningsprosessen. Mens trilogforhandlingen ikke har dokumenter på hvordan forhandlingene foregikk, grunnet dens art som uformelle forhandlinger,[190] er det ikke fjerntliggende å legge til grunn at tilleggsvilkårene ble fremforhandlet primært politisk og som et resultat av kompromisser, fremfor grundige faglige vurderinger. Det fremstår heller ikke som at lovendringen har vært et hovedfokus under forhandlingene eller lovgivningsprosessen generelt. De konkrete forandringene er ikke særskilt nevnt hverken før eller etter forhandlingene. De fremstår heller å ha vært et sidefokus hvor parlamentsmedlemmer i Europaparlamentet har vært fanebærere. At parlamentsmandatet under trilogforhandlingene ofte klarer å fremme synspunkter som strider mot ekspertranbefalinger, og at rådsmandatet til slutt aksepterer dette, er ikke et ukjent fenomen.[191]

[188] EUR-Lex, «Trilogue», *EUR-Lex*, u.å. [Tilgjengelig: https://eur-lex.europa.eu/EN/legal-content/glossary/trilogue.html] (lest 04.09.2024).
[189] Interinstitusjonelle forhandlinger – Trilog av 2. og 3. oktober 2023, s. 353.
[190] Brandsma (2019), s. 1465.
[191] Roederer-Rynning og Greenwood (2015), s. 16 og 27.

4.3 KI-forordningen artikkel 59

4.3.1 Innledning

KI-forordningen artikkel 59 (1) gir på samme måte som KI-forordningen artikkel 10 (5) et supplerende rettsgrunnlag for behandling av personopplysninger.[192] Bestemmelsen tar for seg både alminnelige personopplysninger og særlige kategorier av personopplysninger, og er myntet på henholdsvis GDPR artikkel 6 (4) og artikkel 9 (2) bokstav g.[193] Bestemmelsen åpner opp for at personopplysninger den behandlingsansvarlige har samlet inn for andre formål, ved regulatoriske sandkasser kan brukes for «developing, training and testing certain AI systems», jfr. KI-forordningen artikkel 59 (1).

GDPR Artikkel 6 (4) regulerer behandlingen av personopplysninger for andre formål enn de opprinnelig var samlet inn for. Vanligvis skjer dette gjennom en forenlighetsvurdering.[194] I dette tilfellet utgjør derimot KI-forordningen artikkel 59 en unionsrettshjemmel for å behandle personopplysningene for andre formål enn de opprinnelige var samlet inn for. GDPR artikkel 6 (4) åpner etter en antitetisk tolkning opp for dette. Bestemmelsen stadfester nemlig at behandling for andre formål må skje etter en forenlighetsvurdering dersom behandlingen «ikke bygger på […] unionsrett[] […] som utgjør et nødvendig og forholdsmessig tiltak i et demokratisk samfunn for å sikre oppnåelse av målene nevnt i artikkel 23 nr. 1». Det vil gå utenfor oppgavens rammer å overprøve hvorvidt hjemmelen faktisk utgjør dette.

Formålet med disse sandkassene er å legge til rette for «a controlled environment that fosters innovation and facilitates the development, training, testing and validation of innovative AI systems for a limited time before their being placed on the market or put into service», gitt at en følger «a specific sandbox plan agreed between the providers or prospective providers and the competent authority».[195] Slike sandkasser kan involvere tester under virkelige forhold,[196] og skal etableres av de vedkommende myndighetene på et nasjonal nivå.[197] Datatilsynet har lenge benyttet seg av personvernsandkasser for å legge til rette for personvernvennlig innovasjon og digitalisering, til tross for at GDPR ikke har en tilsvarende hjemmel for

[192] Se KI-forordningen fortalepunkt 140.
[193] Ibid.
[194] Skullerud mfl. (2023), Artikkel 6. Behandlingens lovlighet, Juridika [Tilgjengelig: https://juridika.no/no/lov/2016-04-27-679/%C2%A76/kommentar/] (lest 24.09.2024).
[195] KI-forordningen artikkel 57 (5).
[196] KI-forordningen artikkel 57 (5), siste setning.
[197] KI-forordningen artikkel 57 (1).

opprettelse eller bruk av disse.[198] Hovedformålet med en regulatorisk sandkasse er å åpne opp for teknologisk utvikling av nye og potensielt grenseoverskridende KI-systemer, men da innenfor for trygge, isolerte og begrensede rammer. De regulatoriske sandkassene er viktige for å tilrettelegge for innovasjon på et nytt og relativt uutforsket retts- og teknologifelt, uten å krenke enkeltindividers rettigheter.

Som KI-forordningen artikkel 10 (5) stiller KI-forordningen artikkel 59 (1) en rekke vilkår for å benytte seg av det supplerende rettsgrunnlaget. I motsetning til artikkel 10 (5) er disse vilkårene ikke eksplisitt satt opp som *tilleggs*vilkår, men kun som betingelser (EN/DK/SE: conditions/betingelser/villkor) som må etterleves. Ordlyden tilsier – som et utgangspunkt – at dersom man har oppfylt en plikt etter GDPR som har overlapp med en betingelse etter artikkel 59, er det *ikke* nødvendig å gjøre noe mer eller særskilt for å oppfylle et sett med ekstra angitte tilleggsvilkår. Om en betingelse faktisk utgjør et tilleggsvilkår, vil derimot ikke alene basere seg på hvorvidt bestemmelsen uttrykkelig stadfester dette selv, men òg avhenge av dens materielle krav. I det følgende skal disse betingelsene som følger av artikkel 59 gjennomgås med særlig fokus på hvorvidt disse betingelsene – henholdt GDPR – i realiteten utgjør dobbelregulerende tilleggsvilkår, om det foreligger overlapp hvor etterlevelse av GDPR er tilstrekkelig, og om det foreligger andre materielle sider ved betingelsene som på et personvernrettslig plan kan være problematisk.

4.3.2 Offentlig interesse

Den første betingelsen er at KI-systemene i sandkassen skal utvikles for «safeguarding substantial public interest».[199] Ikke alle former for allmenne interesser kan imidlertid påberopes, selv dem som ellers anerkjennes av EU-retten. De allmenne interessene som kan forfølges er allmenn sikkerhet og folkehelsen, høyt beskyttelsesnivå og forbedring av miljøkvaliteten, bærekraftig energi, sikkerhet og robusthet i transportsystem og mobilitet, kritisk infrastruktur og nettverk, og til slutt effektivitet og kvalitet i den offentlige forvalting og offentlige tjenester.[200]

[198] Datatilsynet – «Ferdige prosjekter og rapporter».
[199] KI-forordningen artikkel 59 (1) bokstav a.
[200] Ibid. romertall i-v.

Opplistingen av de allmenne interessene passer godt inn med systematikken som følger av GDPR artikkel 9 (2) bokstav g, ved å konkretisere *spesifikt* hvilke viktige allmenne interesser som det supplerende rettsgrunnlaget er ment å hensynta, fremfor å gjengi at en må forfølge allmenne interesser *generelt*. Bestemmelsen komplementerer dermed det eksisterende personvernregelverket, og gjør det enkelt for deltakere av et sandkasseprosjekt å forstå hvilke rammer det foreligger på formålene som kan forfølges for den videre behandlingen av personopplysninger.

4.3.3 Nødvendig

Den andre betingelsen er at opplysningene som behandles er *nødvendige* for å overholde ett eller flere krav som stilles i KI-forordningen kapittel III del 2, hvor disse kravene ikke kan oppfylles effektivt gjennom behandling av anonymiserte, syntetiske eller andre opplysninger som ikke er personopplysninger.[201] Disse kravene er at et risikostyringssystem skal opprettes, gjennomføres, dokumenteres og vedlikeholdes,[202] at høyrisiko KI som trenes skal utvikles på trenings-, valideringss- og testdatasett som oppfyller gitte kvalitetskrav,[203] at teknisk dokumentasjon utarbeides før omsetning eller bruk, og holdes oppdatert,[204] loggføring,[205] transparens og informering overfor deployers,[206] utviklet med mulighet for menneskelig overvåkning,[207] og at høyrisiko KI-systemer utvikles og designes slik at de har egnende nivåer av nøyaktighet, robusthet og cybersikkerhet.[208]

Noe tilsvarende følger ikke av GDPR, og betingelsen bidrar til å konkretisere i hvilke tilfeller det er mulig å benytte seg av artikkel 59 (1) som et supplerende rettsgrunnlag. En kan likevel se regulatoriske overlapp med dataminimeringsprinsippet slik det følger av GDPR artikkel 5 (1) bokstav c og redegjort for i punkt 4.2.2. Tilsvarende som at prinsippet kan tilsi at en ikke behandler sensitive personopplysninger hvor alminnelige personopplysninger er tilstrekkelige,[209] vil prinsippet også tilsi at en ikke behandler selv alminnelige personopplysninger dersom bruk av ikke-personopplysninger er tilstrekkelig for å oppnå

[201] Ibid. bokstav b.
[202] KI-forordningen artikkel 9 (1).
[203] KI-forordningen artikkel 10 (1).
[204] KI-forordningen artikkel 11 (1).
[205] KI-forordningen artikkel 12 (1).
[206] KI-forordningen artikkel 13 (1) og (2).
[207] KI-forordningen artikkel 14 (1).
[208] KI-forordningen artikkel 15 (1).
[209] Se punkt 4.2.2 for mer om dataminimeringsprinsippet.

formålet. Dataminimeringsprinsippet forplikter altså den behandlingsansvarlige å behandle ikke-personopplysninger dersom behandling av personopplysninger ikke er nødvendig.

Bestemmelsen er derimot bedre tilpasset typetilfellet ved å stadfeste og begrense *hvilke* formål som er relevante. Adgangen til å behandle personopplysninger knyttes opp til kravene og pliktene som påhviler etter KI-forordningen, slik at særkarakterene som foreligger ved høyrisiko KI-systemer reflekteres i betingelsene som stilles. Dette er i samsvar med de «egnede og særlige tiltak[ene]» som kreves av det supplerende rettsgrunnlaget.[210]

4.3.4 Overvåkningsmekanisme

Den tredje betingelsen er at det skal foreligge effektive overvåkningsmekanismer som kan identifisere hvorvidt det under sandkasseeksperimentet forekommer høy risiko for de registrertes rettigheter og friheter «as referred to in Article 35 of [the GDPR]», samt responsmekanismer mot nevnte risikoer.[211]

Som nevnt i punkt 4.2.7 foreligger det allerede en plikt for den behandlingsansvarlige til å foreta konsekvensutredninger dersom behandlingen av personopplysninger vil medføre høy risiko for fysiske personers rettigheter og friheter etter GDPR, jfr. GDPR artikkel 35 (1). Denne trengs derimot kun å utføres *før* behandlingen,[212] eller senere ved behov – eller, dersom behandlingen endres underveis – en ny vurdering for å avdekke hvorvidt behandlingen fortsatt skjer i samsvar med personvernkonsekvensutredningen.[213]

Nytt med KI-forordningen er altså at en må kontinuerlig overvåke behandlingen slik at en kan effektivt oppdage og avbøte disse risikoene løpende mens sandkasseeksperimentet pågår. Dette utvider plikten slik den følger av GDPR artikkel 35, og tilpasser den typesituasjonen og problemene den behandlingsansvarlige kan støte på som følge av bruk av personopplysninger i høyrisiko KI-systemer: nemlig at rammene for behandlingen kan endres hurtig og radikalt. Risikoene identifisert i personvernkonsekvensutredningen kan da fort bli utdaterte og ikke lenger gjenspeile risikoene ved den faktiske behandlingen. Betingelsen fremstår dermed som et tiltak som er særlig egnet typesituasjonen.

[210] Se punkt 4.1.1 og GDPR artikkel 9 (2) bokstav g.
[211] KI-forordningen artikkel 59 (1) bokstav c.
[212] GDPR artikkel 35 (1).
[213] Ibid. (11).

4.3.5 Separat, isolert og beskyttet

Den fjerde betingelsen er at personopplysninger som behandles i forbindelse med sandkassen befinner seg i et funksjonelt *separat*, *isolert* og *beskyttet* databehandlingsmiljø under den potensielle leverandørens kontroll og med adgang kun av autoriserte personer.[214]

At personopplysninger skal være i et funksjonelt separat og isolert databehandlingsmiljø, er ikke et vilkår som kan utledes direkte av GDPR. Dette kan derimot etter GDPR artikkel 32 (1) være et «teknisk[] og organisatorisk[] tiltak» som er nødvendig for å oppnå et «sikkerhetsnivå som er egnet med hensyn til risikoen». At KI-forordningen artikkel 59 setter dette opp som en eksplisitt betingelse, er trolig begrunnet i et ønske om at personopplysninger som brukes i sandkasseeksperimentet ikke skal blandes – eller viderebrukes – med personopplysninger som ikke skal brukes i sandkassen. Hjemmelen til å viderebehandle disse personopplysningene er særegent for den regulatoriske sandkassen og skal ikke benyttes for andre formål enn dette.

At personopplysningene skal være i et *beskyttet* databehandlingsmiljø er derimot ikke et tiltak som er særskilt for KI-tilfellene, og gjelder generelt ved enhver behandling av personopplysninger. Manglende sikkerhet rundt behandlingen av personopplysningene er et brudd på de grunnleggende prinsippene etter GDPR.[215] Se GDPR artikkel 32 (1) og punkt 4.2.3. Bestemmelsen tilføyer altså ingenting her.

At kun autoriserte personer skal ha adgang til personopplysningene, følger også allerede av GDPR. Konfidensialitet i form av hindring av uautorisert adgang er et grunnleggende prinsipp for behandling av personopplysninger,[216] samt et krav for sikkerheten ved behandlingen etter GDPR artikkel 32 (1) bokstav b. For nærmere om dette se punkt 4.2.4. Særreguleringen av konfidensialitetsplikten fremstår dermed som unødvendig, ettersom uautorisert adgang til personopplysningene den behandlingsansvarlige behandler uansett er et brudd på personvernregelverket. Det faktum at personopplysninger behandles i forbindelse med en sandkasse, påvirker ikke konfidensialitetsplikten slik den følger av GDPR.

[214] KI-forordningen artikkel 59 (1) bokstav d.
[215] GDPR artikkel 5 (1) bokstav f.
[216] Ibid.

4.3.6 Deling av data og personopplysninger

KI-forordningen artikkel 59 (1) bokstav e stadfester at deling av data kun kan skje i samsvar med EUs databeskyttelseslovgivning. Betingelsen tilføyer altså ingenting nytt på dette punktet. Den setter likevel en begrensning ved at personopplysninger som er skapt *i* sandkassen, «cannot be shared *outside* the sandbox».[217]

Dette er et særlig tiltak som bidrar med å minske den høye risikoen som er assosiert med bruken av høyrisiko KI. Personopplysningene som skapes i disse sandkassene, har blitt til under eksperimentelle og uutforskede omstendigheter. Opplysningene kan dermed ofte være av «dårlig kvalitet» ved at de ikke nødvendigvis er sanne,[218] eller har blitt behandlet under omstendigheter som hverken oppfattes som rettferdig eller åpen hensyntatt den registrerte.[219] Reguleringen fremstår dermed fornuftig.

4.3.7 Valg overfor de registrerte

Etter KI-forordningen artikkel 59 (1) bokstav f skal behandlingen av personopplysninger i sandkassen hverken føre til tiltak eller valg som påvirker de registrerte, eller påvirke anvendelsen av deres rettigheter, slik de følger av unionens personvernregelverk.

Denne særreguleringen har flere likheter med GDPR artikkel 22 (1), hvor den registrerte har rett til å «ikke å være gjenstand for en avgjørelse» som utelukkende er «basert på automatisert behandling, herunder profilering» og som har «rettsvirkning for eller på tilsvarende måte i betydelig grad påvirker vedkommende».

Bestemmelsen går derimot drastisk lenger enn GDPR artikkel 22 (1). For det første omfatter KI-forordningen artikkel 59 (1) ikke bare «avgjørelse[r]», men også tiltak og valg generelt, så fremt disse påvirker den registrerte. Videre trenger ikke disse tiltakene og valgene å medføre «rettsvirkning» eller «tilsvarende måte i betydelig grad påvirke[] vedkommende» – de trenger bare å påvirke den registrerte. Ordlyden tilsier at det skal svært lite til før de registrerte anses å være påvirket av den behandlingsansvarliges tiltak eller valg. Til slutt er det ikke noe krav om at det er tale om en «automatisert behandling». Mens sistnevnte også – og særlig – hadde gitt mening i en KI-kontekst, ettersom KI-systemer i nyere tid typisk tar nettopp slike automatiserte

[217] KI-forordningen artikkel 59 (1) bokstav e, min kursivering.
[218] GDPR artikkel 5 (1) bokstav d.
[219] GDPR artikkel 5 (1) bokstav a.

avgjørelser,[220] så fanger bestemmelsen *ethvert* tiltak eller valg overfor de registrerte som angår deres personopplysninger og som skjer i sandkassen. Dette vil da omfatte manuelle, så vel som automatiserte tiltak eller valg.

Det siste delen av betingelsen, at behandlingen av personopplysninger i sandkassen ikke skal påvirke de registrertes rettigheter slik de følger av personvernregelverket, fremstår derimot som overflødig. Bestemmelsen sier mer eller mindre at man skal følge loven, hvilket skal være unødvendig. Det kan tenkes at dette er en konsekvens av ordlyden i KI-forordningen artikkel 2 (7), som stadfester at anvendelsen av KI-forordningen ikke skal påvirke GDPR, men «without prejudice to […] Article 59 of this Regulation».[221] I så fall fremstår dette som en uheldig og forvirrende lovreguleringsteknikk, ved å åpne opp for at det kan gjøres unntak, for å deretter utelukke slike unntak i selve lovbestemmelsen.

4.3.8 Tekniske og organisatoriske tiltak samt sletting

KI-forordningen artikkel 59 (1) bokstav g går ut på at behandlingen av personopplysninger skal være beskyttet av egnede tekniske og organisatoriske tiltak, og skal slettes enten når deltakelse i sandkassen er ferdig, eller når personopplysningene har nådd sin lagringstid.

Den første delen av denne betingelsen fremstår som fullstendig overflødig. At den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak, følger allerede av GDPR artikkel 32, og KI-forordningen tilføyer ingenting nytt for den behandlingsansvarliges plikter på dette punktet. Dette fremstår dessuten som unødvendig når det allerede er satt opp som en særskilt betingelse at dataene skal være i et beskyttet databehandlingsmiljø etter bokstav d.[222] Dette vil som poengtert i punkt 4.3.5 være et tiltak som logisk vil falle inn under egnede tekniske og organisatoriske tiltak.

Angående sletting vil de samme betraktningene gjøre seg gjeldende her som ved KI-forordningen artikkel 10 (5) bokstav e.[223] Er deltakelsen i sandkassen ferdig, så er formålet oppnådd eller frafalt, og personopplysningene skal slettes, se GDPR artikkel 17 (1) bokstav a, og artikkel 5 (1) bokstav e og (2). Har personopplysningene nådd sin lagringstid, vil den

[220] Jarbekk og Sommerfeldt (2024), s. 134.
[221] Se punkt 4.2.1 for mer om KI-forordningen artikkel 2 (7).
[222] Se punkt 4.3.5.
[223] Som redegjort for i punkt 4.2.6.

behandlingsansvarlige ha en plikt til å slette dem, se GDPR artikkel 5 (1) bokstav e og (2). Heller ikke her tilfører KI-forordningen altså noe nytt.

4.3.9 «Logs» over behandlingsaktivitetene

Etter KI-forordningen artikkel 59 (1) bokstav h, skal «logs» over behandlingsaktiviteten gjort i sandkassen beholdes under deltakelsen i sandkasseeksperimentet, med mindre annet følger av nasjonal- eller unionsrett.

«[L]ogs» må ikke forveksles med behandlingsprotokoller.[224] Bestemmelsen om behandlingsprotokoller i GDPR artikkel 32 (EN/DK/SE: Records of processing activities/Fortegnelser over behandlingsaktiviteter/Register över behandling) benytter seg av en annen terminologi enn KI-forordningen gjør her (EN/DK/SE: Logs/Logfilerne/Loggarna). Videre benytter KI-forordningen seg direkte av terminologien «records of processing activities» når den henviser til behandlingsprotokoller, eksempelvis ved KI-forordningen artikkel 10 (5) bokstav f.[225]

KI-forordningen definerer ikke «logs»-begrepet i definisjonsartikkelen i artikkel 3, men definerer det i en annen kontekst, nemlig når den stadfester at «[h]igh-risk AI systems shall technically allow for the automatic recording of events (logs) over the lifetime of the system».[226] Til tross for at dette er en mer generell type «logs», gir bestemmelsen en god pekepinn på hva KI-forordningen mener når den ellers benytter seg av begrepet «logs». At en skal drive med «logging», kan være et sikkerhetstiltak som kreves etter GDPR artikkel 32,[227] men dette kan vanskelig oppstilles som en universal forpliktelse for enhver som behandler personopplysninger.

KI-forordningen artikkel 59 (1) bokstav h stiller dermed et krav til behandlingen som ikke stilles av GDPR for øvrig, men som er et godt egnet tiltak for situasjoner hvor man driver med storskala behandling av personopplysninger gjennom omfattende tekniske og kompliserte systemer – som et KI-system.

[224] Som redegjort for i punkt 4.2.7.
[225] Ibid.
[226] KI-forordningen artikkel 12.
[227] Gulbrandsen og Moe (2024), forfatterne tar imidlertid til orde for at logging er «et grunnleggende informasjonssikkerhetstiltak som *skal* være iverksatt» (min kursivering) etter GDPR artikkel 32. Selv om dette er et tiltak som *ofte* vil være aktuelt å benytte seg av, så fremstår det som unyansert å legge til grunn at dette alltid er påkrevd i enhver personopplysningsbehandlingskontekst.

4.3.10 Beskrivelse av behandlingen

Videre er det en betingelse at en fullstendig og detaljert beskrivelse av behandlingen og begrunnelsen for treningen, testingen og valideringen av KI-systemet holdes sammen med testresultatene, som en del av den tekniske dokumentasjonen i bilag IV.[228]

At den behandlingsansvarlige skal ha en beskrivelse av behandlingen, kan delvis utledes av GDPR artikkel 5 (1) bokstav b – personopplysninger skal «samles inn for spesifikke, uttrykkelig angitte […] formål» –, og GDPR artikkel 13 (1) bokstav c – den behandlingsansvarlige skal ved innsamlingen gi informasjon om «formålene med den tiltenkte behandlingen». Informasjonsplikten er derimot myntet på *formålet* og tar ikke direkte for seg *selve behandlingen*. En beskrivelse av selve behandlingen kan imidlertid tenkes å være naturlig når en beskriver formålet. Datatilsynet rubriserer eksempelvis informasjon om formålet som et underpunkt av informasjon om behandlingen,[229] og WP29-gruppen har lagt til grunn at formålsbeskrivelsen må være såpass detaljert at det er mulig for den registrerte å dedusere hvilke behandlinger som omfattes og som ikke omfattes av formålet,[230] samt at en ytterligere detaljert beskrivelse av personopplysningsbehandlingen kan gis til dem som trenger det.[231] KI-forordningen går likevel på dette punktet lenger enn GDPR, ved å gjøre det uttrykkelig klart at det er selve personopplysningsbehandlingen som skal beskrives. GDPR fortalepunkt 60 understøtter dette, og understreker at prinsippene om rettferdig og åpen behandling krever at de registrerte «informeres om at behandlingen *skjer*, samt om *formålet* med den»,[232] *ikke* at det gis en beskrivelse av selve behandlingen.

Plikten etter KI-forordningen må derimot ses i lys av at denne informasjonen er ment for *vedkommende myndighet*, ikke den *registrerte*. KI-forordningen artikkel 11 stiller krav om at det skal foreligge teknisk dokumentasjon slik at leverandører av KI-systemer kan demonstrere overfor vedkommende myndighet at deres høyrisiko KI-systemer etterlever kravene i del 2 av KI-forordningen.[233] Hva som kreves av teknisk dokumentasjon fremkommer av bilag IV,[234] hvor EU-kommisjonen i løpet av en femårsperiode fra 1. august 2024 har adgang til å foreta

[228] KI-forordningen artikkel 59 (1) bokstav i.
[229] Datatilsynet – «Hva skal virksomheten gi informasjon om?».
[230] Artikkel 29-gruppen – Uttalelse 03/2013 (2013), s. 15.
[231] Ibid. s. 16 og tilsluttet av Voigt og von dem Bussche (2024), s. 138.
[232] Mine kursiveringer.
[233] KI-forordningen artikkel 11 (1).
[234] KI-forordningen bilag IV.

løpende tilpasninger av kravene for teknisk dokumentasjon.[235] Det gjør seg dermed gjeldende andre hensyn ved viderebehandling av personopplysninger i KI-sandkasser enn det gjør ved behandling av personopplysninger generelt, hvilket bestemmelsen på dette punktet reflekter.

Videre har GDPR et grunnprinsipp om at den behandlingsansvarlige skal ansvarliggjøres og påvise overholdelse av forordningen gjennom hele behandlingen.[236] Plikten kan *trolig* tolkes slik at en også skal gi en beskrivelse av behandlingen. Skullerud mfl. tar bl.a. til orde for at «[e]tterlevelse [av plikten] vil kunne påvises gjennom et godt internkontrollsystem, som blant annet beskriver hvilke opplysninger som behandles for hvilke formål, og ikke minst *hvordan opplysningene behandles*».[237] Dette er imidlertid kun et eksempel på hvordan etterlevelse *kan* gjøres, ikke hva GDPR krever. Plikten er såpass generell og situasjonsavhengig at en konkretisering er nødvendig for å stadfeste plikten på en entydig måte, dersom lovgiver ønsker at den alltid skal gjelde i en gitt behandlingssituasjon.

Er KI-systemet som skal testes i sandkassen et høyrisiko KI-system, foreligger det derimot en plikt for den behandlingsansvarlige til å gi en «systematisk beskrivelse» av de planlagte behandlingsaktivitetene i en DPIA.[238] Artikkel 59 er derimot myntet på *alle* typer KI-systemer, ikke kun høyrisiko. Plikten vil dermed ikke alltid gjøre seg gjeldene. Betingelsen passer dermed godt til særtilfellet.

4.3.11 Kort sammenfatning

Den siste betingelsen er at en kort oppsummering av sandkasseprosjektet, dets mål og forventede resultater blir publisert på vedkommende myndighets nettsider.[239] Denne betingelsen har ikke noen tilsvarende reguleringer etter GDPR, og er en betingelse som bidrar med transparens overfor de registrerte og andre interesserte om hva sandkassen og den medfølgende personopplysningsbehandlingen innebærer.

[235] KI-forordningen artikkel 11 (3) og artikkel 97 (1) og (2).
[236] GDPR artikkel 5 (2) og 24 (1).
[237] Skullerud mfl., Personvernforordningen. Lovkommentar, Artikkel 5. Prinsipper for behandling av personopplysninger, Juridika [Tilgjengelig: https://juridika.no/no/lov/2016-04-27-679/%C2%A75/kommentar/] (lest 11.11.2024), min kursivering.
[238] Se GDPR artikkel 35 (7) bokstav a og punkt 4.2.7.
[239] KI-forordningen artikkel 59 (1) bokstav j.

5 Avsluttende refleksjoner

Som redegjort for i punkt 4.2 og 4.3, foreligger det store overlapp mellom de eksisterende forpliktelsene som stilles etter personvernforordningen, og forpliktelsene som stilles av de supplerende rettsgrunnlagene for behandling av særlige kategorier av personopplysninger i KI-forordningen. Både artikkel 10 (5) og 59 dobbeltregulerer unødvendig flere forpliktelser som følger av GDPR. Bestemmelsene befinner seg likevel langt fra hverandre med tanke på *hvor mye* de lovteknisk kolliderer med personvernregelverket. Artikkel 59 fremstår i større grad enn artikkel 10 (5) som tilpasset den typesituasjonen den er ment å regulere, og er lovteknisk i større grad i harmoni med det eksisterende personvernregelverket, samt hjemmelskravene som stilles til det supplerende rettsgrunnlaget i GDPR artikkel 9 (2) bokstav g.

KI-forordningen artikkel 10 (5) har unødvendige overlapp, forpliktelser som fra et behandlingsansvarligperspektiv er praktisk umulig å etterleve, og innskrenkninger som unødvendig vanskeliggjør behandlingen, samt fremsetter disse som tilleggsvilkår som etter ordlyden må tolkes og anvendes selvstendig fra de tilsvarende reguleringene etter GDPR. I motsetning passer artikkel 59 i større grad med hjemmelskravene som er satt av GDPR artikkel 9 (2) bokstav g, og mer sømløst med forpliktelsene etter GDPR for øvrig. Likevel med noen regulatoriske svakheter. Artikkel 10 (5) kunne i stor grad holdt seg til å fungere som et supplerende rettsgrunnlag, og overlatt sikkerhetstiltakene til GDPR, uten at dette negativt ville påvirket personopplysningsbehandlingssikkerheten rundt hjemmelsgrunnlaget.

Denne lovtekniske skjevheten har trolig sammenheng med at artikkel 59, til forskjell fra artikkel 10 (5), har gjennomgått få endringer i løpet av lovgivningsprosessen siden det opprinnelige forslaget ble lagt frem av EU-kommisjonen. De få endringene som er gjort er enten for å knytte bestemmelsen med de øvrige forandringene ellers gjort med KI-forordningen i løpet av lovgivningsprosessen, eller er små semantiske endringer eller ytterligere henvisninger til det eksisterende personvernregelverket.[240]

Den eneste større forandringen av særlig materiell betydning er gjort i KI-forordningen artikkel 59 bokstav e. Her har EU-lovgiver gått *vekk* fra at enhver personopplysning som blir behandlet ikke kan bli «transmitted, transferred or otherwise accessed by other parties» – tilsvarende som

[240] Sammenlign EU-kommisjonens forslag artikkel 54 og KI-forordningen artikkel 59.

etter den vedtatte artikkel 10 (5) bokstav d –[241] og *heller* gått for den nåværende løsningen slik den er redegjort for i punkt 4.3.6. Deling kan kun skje i samsvar med det eksisterende personvernregelverket, og personopplysninger skapt i sandkassen kan ikke deles utenfor sandkassen. Dette er en løsning som i større grad passer med det eksisterende regelverket.

Etter artikkel 59 har det allerede fra det opprinnelige lovforslaget vært et regulatorisk «skjelett» som de forskjellige etterkommende lovaktørene under lovgivningsprosessen har hatt muligheten å bygge videre på.[242] Etter artikkel 10 har aktørene – og da særlig EU-parlamentet – trolig sett seg nødt til å bygge opp «skjelettet» fra bunnen av, ettersom EU-kommisjonens opprinnelige artikkel 10 (5) nøyde seg med å henvise og gjengi de eksisterende forpliktelsene etter GDPR, med noen få tilpassede presiseringer. Svakhetene som preger artikkel 10 (5) har da trolig oppstått som en konsekvens av sene tilskudd til KI-forordningen, som etter alt å dømme har vært mer politisk enn rettsfaglig styrt.[243]

Mens KI-forordningen ikke er ment å medføre forandringer til det eksisterende regelverket, foreligger det som redegjort for uheldige formuleringer og krav som negativt påvirker reguleringen av behandlingen av særlige kategorier av personopplysninger der disse krysser med kunstig intelligens. Mens KI-forordningen naturlig nok har hatt sitt regulatoriske fokus på kunstig intelligens, er det likevel ugunstig at EU-lovgiver ikke i større grad har hensyntatt de personvernmessige aspektene på en bedre og mer systematisk måte. Særlig når disse har ligget såpass latent. Faren for slike uheldige regulatoriske overlapp med GDPR og KI-forordningen har blitt påpekt av Mario Draghi i hans rapport om europeisk konkuranseevne å være et underliggende systematisk problem, og har i lys av dette tatt til orde for å fjerne disse overlappene.[244] Når bestemmelsene direkte henspiller på eksisterende reguleringer i GDPR, og omhandler såpass sentrale og viktige aspekter som tryggheten rundt behandlingen av særlige kategorier av personopplysninger – især artikkel 10 (5) som tar for seg mottiltak mot skjevheter i høyrisiko KI-systemer – er det bemerkelsesverdig at reguleringen ikke skjer på en mer oversiktlig, håndhevbar og harmoniserende måte.

[241] Se punkt 4.2.5.
[242] Sammenlign det opprinnelige forslaget artikkel 54.
[243] Som redegjort for i punkt 4.2.8.
[244] Europakommisjonen, «The future of European competitiveness Part B | In-depth analysis and recommendations», *Europakommisjonen*, 9. september 2024, s. 79 [Tilgjengelig: https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en?filename=The%20future%20of%20European%20competitiveness_%20In-depth%20analysis%20and%20recommendations_0.pdf] (lest 27.11.2024).

Dette er desto mer problematisk fra et norsk rettsregulatorisk perspektiv. Norge har, til tross for sitt sterke initiativ på personvern- og KI-rettsfeltet, ikke hatt særlig mulighet til å påvirke lovgivningsprosessen, og dermed er prisgitt EUs regulatoriske utforming av KI-forordningen.

Disse gapene vil imidlertid trolig ikke komme på spissen i praksis. Det er nærliggende å legge til grunn at de behandlingsansvarlige – da særlig i artikkel 10 (5)-tilfeller – uutfordret vil falle tilbake på løsninger som ligger nærmest dem som allerede er gjeldende på personvernrettsfeltet. Ved eventuelle tvister overfor domstolen vil man trolig se seg nødt til å tolke KI-forordningen på en måte som harmoniserer artikkel 10 (5) og 59 bedre med GDPRs etablerte personvernsystematikk. Å måtte løse slike regulatoriske svakheter gjennom domstolene er imidlertid ugunstig, og understreker at KI-forordningen og kravene som stilles der burde vært mer hensiktsmessig utformet ved krysningspunktet med personvernforordningen.

6 Litteraturliste

6.1 Norsk rett

6.1.1 Norske lover og forarbeider

Gamle personopplysningsloven — Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).

Prop. 56 LS (2017–2018) — Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen.

Personopplysningsloven — Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven).

6.1.2 Forvaltningsorgan og tilsynsmyndigheter

Datatilsynet – «Ferdige prosjekter og rapporter» — Sandkassesiden – Ferdige prosjekter og rapporter, u.å.

Tilgjengelig:

https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/ferdige-prosjekter-og-rapporter/ (lest 12.09.2024).

Kommunal- og moderniseringsdepartementet – Holdningsdokument KI-forordningen — 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), u.å.

Tilgjengelig:

https://www.regjeringen.no/contentassets/939c260c81234eae96b6a1a0fd32b6de/norwegian-position-paper-on-the-ecs-proposal-for-a-regulation-of-ai.pdf (lest 19.08.2024).

Datatilsynet – «Kunstig intelligens og personvern»

Rapporter og utredninger – Kunstig intelligens og personvern, 11. januar 2018.

Tilgjengelig:

https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/kunstig-intelligens/ (lest 23.08.2024).

Datatilsynet – «Hva er en databehandler?»

Virksomhetenes plikter – Behandlingsansvarlig og databehandler – Hva er en databehandler?, 17. juli 2019.

Tilgjengelig:

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsansvarlig-og-databehandler/hva-er-en-databehandler/ (lest 31.10.2024).

DFØ-rapport 2024:9

DFØ-rapport 2024: 9 august 2024 Forvaltningsstruktur for KI-forordningen.

Tilgjengelig:

https://dfo.no/sites/default/files/2024-08/DF%C3%98-rapport%202024-9%20Forvaltningsstruktur%20for%20KI-forordningen.pdf (lest 05.10.2024).

Datatilsynet – «Hva skal virksomheten gi informasjon om?»

Virksomhetenes plikter – Informasjon og åpenhet – Hva skal virksomheten gi informasjon om?, sist endret 27. juli 2023.

Tilgjengelig:

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjon-og-apenhet/hva-skal-virksomheten-gi-informasjon-om/ (lest 10.11.2024).

6.2 EU-rett

6.2.1 Dommer fra EU-domstolen

***OT [GC]* C-184/20**

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

***Pankki S [C5]* C-579/21**

Dom av 22. Juni 2023 [C5], *J.M. intervening parties: Apulaistietosuojavaltuutettu, Pankki S* C-579/21, EU:C:2023:501.

***Meta Platforms Inc [GC]* C-252/21**

Dom av 4. juli 2023 [GC], *Meta Platforms Inc and Others v Bundeskartellamt*, C-252/21, EU:C:2023:537.

***VB [C5]* C-340/21**	Dom av 14. desember 2023 [C5], *VB v Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986.
***MediaMarktSaturn [C5]* C-687/21**	Dom av 25. januar 2024 [C5], *BL v MediaMarktSaturn Hagen-Iserlohn GmbH [C5]* C-687/21, EU:C:2024:72.
***IAB Europe [C5]* C-604/22**	Dom av 7. mars 2024 [C5], *IAB Europe mot Gegevensbeschermingsautoriteit*, C-604/22, EU:C:2024:214.

6.2.2 Traktater og konvensjoner

Charter of fundamental rights	CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION (2012/C 326/02).
Treaty on the Functioning of the European Union (TFEU)	CONSOLIDATED VERSION OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION (2012/C 326/01).

6.2.3 Direktiver og forordninger

Direktiv (EF) 95/46	DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
Forordning (EU) 2016/679 (GDPR)	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Forordning (EU) 2018/1725 (EUDPR)	REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
Forordning (EU) 2024/1689 (AI-Act)	REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

6.2.4 Lovforarbeid

Europakommisjonen – Forslag til KI-forordningen	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCILLAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, 21. April 2021. Tilgjengelig: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021SC0084 (lest 27.08.2024).

Europakommisjonen – Impact Assessment	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the 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, 21. April 2021. Tilgjengelig: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021SC0084 (lest 07.10.2024).
Europakommisjonen – Explanatory Memorandum	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; EXPLANATORY MEMORANDUM, 21. April 2021. Tilgjengelig: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 (lest 28.08.2024).
Det europeiske parlament – Utkast til betenkning, 20. april 2022	***I DRAFT REPORT on the proposal for a regulation of the European Parliament

	and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM2021/0206 – C9-0146/2021 – 2021/0106(COD)), 20. April 2022. Tilgjengelig: https://www.europarl.europa.eu/doceo/document/CJ40-PR-731563_EN.pdf (lest 27.08.2024).
Det europeiske parlament – Endringsforslag 1581-2005, 13. juni 2022	AMENDMENTS 1581 - 2005 Draft report Brando Benifei, Dragoş Tudorache, 13. juni 2022. Tilgjengelig: https://www.europarl.europa.eu/RegData/commissions/libe/projet_rapport/2022/732839/amendements/CJ40_AM(2022)732839_EN.pdf (lest 01.09.2024).
Det europeiske parlament – Betenkning, 22. mai 2023	***I REPORT on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), 22. mai 2023. Tilgjengelig:

https://www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2023/0188/P9_A(2023)0188_EN.pdf (lest 01.09.2024).

Det europeiske parlament – Vedtatte endringer, 14. juni 2023

Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), 14. juni 2023.

Tilgjengelig:

https://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/definitif/2023/06-14/0236/P9_TA(2023)0236_EN.pdf (lest 01.09.2024).

Interinstitusjonelle forhandlinger – Trilog av 18. juli 2023

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS 2016/0106(COD) [Version for Trilogue on 18 July, 2023] 14-07-2023 at 21h36, 18. juli 2023.

Tilgjengelig:

https://www.europarl.europa.eu/RegData/publications/trilogue/2021/0106/NEGO_CT(2021)0106(2023-07-14)_XL.pdf (lest 03.09.2024).

Interinstitusjonelle forhandlinger – Trilog av 2. og 3. oktober 2023

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 2021/0106(COD) [Version for Trilogue on 2 and 3 October, 2023] 28-09-2023 at 19h18, 3. oktober 2023.

Tilgjengelig:

https://www.europarl.europa.eu/RegData/publications/trilogue/2021/0106/NEGO_CT(2021)0106(2023-10-03)_XL.pdf (lest 03.09.2024).

Rådet for Den europeiske union – Endelig kompromisstekst

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 - Analysis of the final compromise text with a view to agreement, 26. januar 2024.

Tilgjengelig:

https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf (lest 03.09.2024).

6.2.5 Bindende beslutninger, uttalelser, veiledninger og retningslinjer

Artikkel 29-gruppen – Uttalelse 4/2007 (2007)

«Opinion 4/2007 on the concept of personal data», 20. juni 2007.

Tilgjengelig:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec11(lest 22.08.2024).

Artikkel 29-gruppen – Uttalelse 03/2013 (2013)

«Opinion 03/2013 on purpose limitation», 2. april 2013.

Tilgjengelig:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (lest 05.12.2024).

Artikkel 29-gruppen – Retningslinje (2017)

«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», 4. oktober 2017.

Tilgjengelig:

https://ec.europa.eu/newsroom/article29/items/611236/en (lest 09.09.2024).

EDPB – Retningslinje 04/2019	«Guidelines 4/2019 on Article 25 Data Protection by Design and by Default» – Version 2.0, 20. oktober 2020. Tilgjengelig: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en (lest 07.09.2024).
EDPB – Retningslinje 07/2020	«Guidelines 07/2020 on the concepts of controller and processor in the GDPR» – Version 2.1, 7. juli 2021. Tilgjengelig: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en (lest 28.08.2024).
EDPB og EDPS – Felles uttalelse 05/2021	«EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)», 18. Juni 2021. Tilgjengelig: https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en (lest 04.12.2024).

6.3 Juridisk litteratur

6.3.1 Bøker

Fredriksen og Mathisen (2022) Halvard Haukeland Fredriksen og Gjermund Mathisen, EØS-rett, 4. utgave, Fagbokforlaget 2022.

Jarbekk og Sommerfeldt (2024) Eva Jarbekk og Simen Sommerfeldt, Personvern og GDPR i praksis, 2. utgave, Cappelen Damm Akademisk 2024.

Kuner mfl. (2020) Christopher Kuner mfl., The EU General Data Protection Regulation (GDPR) A Commentary, 1. utgave, Oxford University Press 2020.

Voigt og von dem Bussche (2024) Paul Voigt og Axel vom dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide, 2. utgave, Springer 2024.

6.3.2 Artikler

Bekkum (2024) Marvin van Bekkum, «Using sensitive data to debias AI systems: Article 10(5) of the EU AI Act», *Cornell University*.

Tilgjengelig:

https://doi.org/10.48550/arXiv.2410.14501 (lest 27.11.2024).

Brandsma (2019) Brandsma, Gijs Jan, «Transparency of EU informal trilogues through public feedback in the European Parliament: promise

unfulfilled», *Journal of European public policy*, 26, 10 (2019) s. 1464-1483.

Tilgjengelig:

https://doi.org/10.1080/13501763.2018.1528295 (lest 08.10.2024).

Gulbrandsen og Moe (2024)

Hanne Pernille Gulbrandsen og Ole Martin Moe, «Lov, logging, lagring og lengde – Logging som sikkerhetstiltak etter GDPR», *Lov&Data*, 25. juni 2024.

Tilgjengelig:

https://lod.lovdata.no/article/2024/06/Logging%20som%20sikkerhetstiltak%20etter%20GDPR (lest 13.11.2024).

Roederer-Rynning og Greenwood (2015)

Roederer-Rynning, Christilla og Greenwood, Justin, «The culture of trilogues», *Journal of European public policy*, 22, 8 (2015) s. 1148-1165.

Tilgjengelig:

https://doi.org/10.1080/13501763.2014.992934 (lest 08.10.2024).

6.3.3 Lovkommentarer

Skullerud mfl. (2023)

Åste Marie Bergseng Skullerud mfl., Personvernforordningen (GDPR) – Kommentarutgave, i Juridika, 2018, ajourført 1. april 2023.

6.4 Andre kilder

6.4.1 Internettadresser

Det Europeiske parlament, «Artificial Intelligence Act: MEPs adopt landmark law», *Det Europeiske parlament*, 13 mars 2024, tilgjengelig: https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law (lest 15.08.2024).

EUR-Lex, «Trilogue», *EUR-Lex*, u.å., tilgjengelig: https://eur-lex.europa.eu/EN/legal-content/glossary/trilogue.html (lest 04.09.2024).

Europakommisjonen, «The future of European competitiveness Part B | In-depth analysis and recommendations», *Europakommisjonen*, 9. september 2024, s. 79, tilgjengelig: https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en?filename=The%20future%20of%20European%20competitiveness_%20In-depth%20analysis%20and%20recommendations_0.pdf (lest 27.11.2024).

European Data Protection Board, «Endorsed WP29 Guidelines», *edpb.europa.eu*, tilgjengelig her: https://www.edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en (lest 20.08.2024).

Jeremy White, «How Strangers Got My Email Address From ChatGPT's Model», *The New York Times*, 22 desember 2023, tilgjengelig: https://www.nytimes.com/interactive/2023/12/22/technology/openai-chatgpt-privacy-exploit.html (lest 16.08.2024).

Matt Burgess, «ChatGPT Has a Big Privacy Problem», *Wired*, 4 april 2023, tilgjengelig: https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/ (lest 15.08.2024).

Regjeringen, «Forslag til forordning om kunstig intelligens (KI-forordningen)», *Regjeringen.no*, 29 januar 2024, tilgjengelig: https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/juni/forslag-til-forordning-om-kunstig-intelligens-ki-forordningen/id2884935/ (lest 19.08.2024).

Rådet for Den europeiske union, «Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights», *Rådet for Den europeiske union*, 6. desember 2022, Tilgjengelig: https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/ (lest 03.09.2024).