Høringsuttalelse - forslag til ny personopplysningslov

1. Innledning

Direktoratet for e-helse viser til høringsbrev av 6. juli 2017 om forslag til ny personopplysningslov, som gjennomfører EUs personvernforordning i norsk rett.

En forutsetning for digitalisering i helse- og omsorgssektoren er godt personvern og forsvarlig IKT-sikkerhet. Innbyggerne og helsepersonell må ha tillit til at de digitale tjenestene fungerer, er tilgjengelige ved behov og har tilstrekkelig sikkerhet. Videre må innbygger på en enkel måte kunne utøve sine rettigheter. Dette er del av den strategiske retningen for digitalisering av helse- og omsorgstjenesten som er beskrevet i Nasjonal e-helsestrategi for 2017-2022[1].

Direktoratet mener at det nye regelverket gir en god ramme for vern av personopplysninger:

- Forordningen har satt personvern og informasjonssikkerhet på dagsorden og har bidratt til bevissthet og økt forståelse av krav til vern av helseopplysninger ved digitalisering av tjenester hos virksomheter i helse- og omsorgstjenesten.
- Forordningen styrker innbyggers rettigheter, noe som i stor utstrekning sammenfaller med målet om pasientens digitale helsetjeneste.
- Forordningen trekker frem bruk av «soft-law» og bransjenormer for etterlevelse av regelverk, noe som vi har positiv erfaring med fra arbeidet med Norm for informasjonssikkerhet i helse- og omsorgssektoren.[2]
- Forordningen innebærer harmonisering som gjør det enklere for internasjonale leverandører av e-helseløsninger å tilpasse seg regelverket og dermed sikre større utvalg av løsninger og mer konkurranse i det norske markedet. Tilsvarende vil norske leverandører lettere kunne tilby sine løsninger i EU.

Direktoratet har valgt å avgrense høringssvaret til tema som berører e-helseområdet.

[1] https://ehelse.no/strategi/e-helsestrategi
[2] https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet

Direktoratet for e-helse
E-helse Avdeling juridisk
Siri Pernille Utkilen, tlf.: 93609505
Postboks 6737 St. Olavs plass, 0130 OSLO • Besøksadresse: Verkstedveien 1 • Tlf.: 21 49 50 70
Org.nr.: 915 933 149 • postmottak@ehelse.no • www.ehelse.no

2. Innspill til utkast til lov om behandling av personopplysninger

Direktoratet for e-helse støtter i hovedsak departementets forslag til ny personopplysningslov. Vi vil likevel knytte kommentarer til enkelte av lovbestemmelsene i forslaget.

Generelt støtter direktoratet forslaget om at nasjonale, generelle og supplerende bestemmelser gis i den nye personopplysningsloven, mens sektorspesifikke regler gis i særlovgivningen. Behandling av helseopplysninger i helse- og omsorgstjenesten har behov for et særskilt vern og reguleres også i dag i stor grad i særlovgivningen. Vi viser til Helse- og omsorgsdepartementets arbeid med tilpasninger i helselovgivningen som følge av forordningen.

Utkast § 7 Behandling av sensitive personopplysninger som er nødvendig av hensyn til viktige samfunnstjenester

Direktoratet støtter at Datatilsynet gis adgang til å gjøre unntak fra forbudet i artikkel 9 nr. 1 i særlig tilfeller når viktige samfunnsinteresser tilsier dette, jf. lovutkastet § 7. Direktoratet mener at det også i fremtiden vil kunne oppstå særlige og uforutsette behov for behandling av helseopplysninger som er nødvendig av hensyn til viktige samfunnsinteresser, uten at det er tid til eller naturlig å vedta lovgivning som regulerer behandlingen. Direktoratet mener derfor at det er behov for en slik «sikkerhetsventil» som departementet foreslår.

Utkast § 9 Bruk av fødselsnummer og andre entydige identifikasjonsmidler

Direktoratet støtter en fortsatt restriktiv bruk av fødselsnummer, jf. lovutkastet § 9. Bakgrunnen for dette er at helsesektoren bruker fødselsnummeret som en primærnøkkel i de aller fleste pasientsystemer, for å finne frem til riktig person og deres personopplysninger. Dersom fødselsnumrene blir lettere tilgjengelig vil det kunne medføre at uvedkommende lettere kan få tilgang til andres helseopplysninger.

I vår sektor ville en mindre restriktiv beskyttelse av fødselsnummer kunne medføre betydelige rutineendringer for hvordan bruk av fødselsnummer skal håndteres. Direktoratet viser til en utdypende behandling av denne problemstillingen i vår høringsuttalelse om «Forslag til ny personidentifikator» fra juni 2017 [3] og de tidligere høringsuttalelsene som er referert i denne høringsuttalelsen. Her vises det blant annet til hvordan fødselsnummeret blir brukt i samhandlingen mellom pasient, helseaktører og pasientsystemer.

Utkast § 10 Overføring av personopplysninger til tredjestater

Direktoratet støtter departementets forslag om at kongen kan gi bestemmelser om overføring av personopplysninger til utlandet, jf. lovutkastet § 10 andre ledd. Vi støtter departementets vurdering om å holde åpent muligheten for å kunne forskriftsregulere og fastsette begrensninger for overføring av sensitive personopplysninger til utlandet.

[3] https://ehelse.no/Documents/E-helsekunnskap/H%c3%b8ringsuttalelse_forslag_ny_personidentifikator_PID_pdf.pdf

Utkast § 11 Forhåndsdrøftinger

Direktoratet støtter en forskriftshjemmel som kan brukes til nærmere regulering av plikten til forhåndsdrøfting, lovutkastet § 11. Vi mener at det bl.a. kan være nødvendig å presisere hvilke typer behandlinger som krever forhåndsdrøftinger.

Vi vil imidlertid peke på en praktisk utfordring rundt dette med forhåndsdrøftinger og bruk av «smidig» metodikk i utviklingsprosjekter. «Smidig» metodikk legger opp til at løsningen skisseres underveis i utviklingen, mens en forhåndsdrøfting skal foretas i forkant. En konsekvens er da at det kan være vanskelig å foreta forhåndsdrøftinger på noe annet enn et konseptuelt nivå.

Videre mener vi at listen for hvilke saker som krever forhåndsdrøfting ikke må legges for lavt, slik at det fører til unødig stor saksmengde og lange saksbehandlingstider.

Utkast § 11 Forhåndsgodkjenning

Direktoratet støtter departementets vurderinger om at plikten til å innhente forhåndsgodkjennelse (konsesjon) fra Datatilsynet ikke videreføres. Bortfall av konsesjonsplikt bidrar også til forenkling. Vi støtter vurderingene om at de nye virkemidlene i forordningen, bl.a. vurdering av personvernkonsekvenser og forhåndsdrøftinger med tilsynsmyndigheten, vil kunne tilrettelegge for at reglene i forordningen overholdes. Vi mener imidlertid at de samme vurderingene må kunne legges til grunn for behandling av helseopplysninger, og at det derfor heller ikke på dette området er behov for forhåndsgodkjenning/konsesjon fra Datatilsynet. I tillegg er vi bekymret for at det vil gi dårlig forutberegnelighet for virksomhetene dersom det legges opp til en ordning med forhåndsgodkjenning/konsesjon kun på enkelte områder. Vi mener derfor at det ikke bør innføres en forskriftshjemmel som kan benyttes til å gjeninnføre forhåndsgodkjenning fra Datatilsynet, jf. lovutkastet § 11.

Utkast § 13 Unntak fra retten til informasjon og innsyn

Direktoratet er positive til det nye regelverket som styrker den registrertes rettigheter. Det tilbys i dag digitale tjenester via portalen «Min helse» på helsenorge.no, som tilrettelegger for at innbygger på en enkel måte kan utøve sine rettigheter overfor helse- og omsorgssektoren.

Direktoratet støtter videreføring av gjeldende rett om begrensninger i innsynsretten og informasjonsplikten, jf. lovutkastet § 13 1 ledd bokstav c). Unntaket er i stor grad sammenfallende med pasientjournalloven § 18, som viser til pasient- og brukerrettighetsloven § 5-1 og helsepersonelloven § 41. Bestemmelsene åpner i særlige tilfeller for å gjøre unntak fra retten til informasjon og innsyn.

Direktoratet mener at det er vanskelig per i dag å overskue og å skulle uttale seg om behovet for unntaksregler fra de øvrige rettighetene. Når det gjelder retten til dataportabilitet vil den kun få anvendelse i begrenset grad på dagens e-helseløsninger. Vi forutsetter at retten til dataportabilitet ikke vil gjelde for Kjernejournal og Reseptformidleren, eller for elektroniske pasientjournalsystemer (EPJ-systemer). Vi vil imidlertid peke på behovet for felles standarder for å ivareta retten til dataportabilitet på en god måte.

Utkast kapittel 5 om personvernrådgiver

Direktoratet mener at begrepet "personvernombud" fortsatt bør benyttes fordi det er et godt innarbeidet begrep i helse- og omsorgssektoren. Dersom man i oversettelsen skal benytte et annet

begrep, mener vi at det er viktig at begrepet tydelig gjenspeiler den utvidede rollen som ordningen får i forordningen.

Utkast § 18 Personvernnemnda

Departementet ber om tilbakemelding på om Personvernnemnda bør reduseres fra 7 til 5 medlemmer. Direktoratet mener at Personvernnemnda fortsatt bør oppnevnes med 7 medlemmer som i dag, og at departementets tidligere begrunnelse for nemndas brede sammensetning står seg. Helse- og omsorgssektoren er en stor sektor med ca. 17 000 små og store aktører som behandler store mengder sensitive personopplysninger på flere nivåer og til mange ulike formål, f. eks i forbindelse med pasientbehandling, i ulike helseregistre og i helseforvaltningen. Dette betyr at problemstillingene som reises på personvernfeltet i vår sektor ofte er komplekse og krever god forståelse for helseområdet. Direktoratet mener derfor at Personvernnemnda fortsatt bør ha 7 medlemmer, og at det bør tas hensyn til bredde og kompetanse i sammensetningen, herunder at nemnda har et medlem som kjenner helseområdet godt.

3. Generelle kommentarer

Norm for informasjonssikkerhet i helse- og omsorgssektoren

Direktoratet mener det er positivt at forordningen peker på «soft-law» mekanismer som sertifisering og bransjenormer for å sikre etterlevelse av nytt personvernregelverk. Det vil kreve fokus og veiledning fra Datatilsynet for å få disse mekanismene til å fungere godt.

Helse- og omsorgssektoren har i over 10 år hatt en bransjenorm for informasjonssikkerhet - Norm for informasjonssikkerhet i helse- og omsorgssektoren («Normen»). Direktoratet for e-helse forvalter sekretariatsfunksjonen for Normen, og vår erfaring er at Normen har bidratt til økt kompetanse og etterlevelse av personvernregelverket i helse- og omsorgstjenesten.

Direktoratet mener at Normen også med nytt personvernregelverk vil kunne bidra til å sikre etterlevelse av de nye personvernreglene og krav til IKT-sikkerhet i helse- og omsorgssektoren. Bruk av bransjenorm kan bli et enda viktigere virkemiddel når de konkrete informasjonssikkerhetsbestemmelsene i personopplysningsforskriften kapittel 2 oppheves. Vi mener at det da blir særlig viktig å kompensere med andre mekanismer, som f. eks. bransjenorm, for å sikre lik forståelse og etterlevelse av krav til informasjonssikkerhet i helse- og omsorgstjenesten. Vår erfaring tilsier at bransjenorm kan være et godt verktøy for å identifisere hva som er «egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen» jf. Art 32 nr. 1, og på den måten bidra til å sikre tilfredsstillende nivå for informasjonssikkerhet i vår sektor.

Bransjenormer, og også antagelig sertifiseringsordninger, vil generelt kunne være gode verktøy for etterlevelse av sikkerhetskrav og for å oppnå et godt personvern. Videre kan de bidra til digitalisering gjennom bl.a. forutsigbarhet i utvikling av teknologi og god leverandøroppfølging.

Behov for veiledning:

Samtykke

Direktoratet mener det er positivt at samtykke opprettholdes som et rettsgrunnlag for behandling av personopplysninger, herunder sensitive personopplysninger. Samtykke er et nødvendig rettsgrunnlag

for å kunne digitalisere og utvikle digitale innbyggertjenester som ikke er regulert i lov. Direktoratet ser at det på noen områder kan være utfordrende å opprettholde et gyldig samtykke over tid, særlig der det trinnvis utvikles nye digitale tjenester. Grensene for hvor mye funksjonalitet som kan legges til i en løsning før samtykke ikke lenger kan sies å være gyldig, oppleves som utfordrende i praksis. Vi mener det er behov for veiledning rundt bruk av samtykke som rettsgrunnlag etter det nye personvernregelverket.

Melding/underretning om brudd på personopplysningssikkerheten

Direktoratet mener det er positivt at behandlingsansvarlig får en utvidet melde- og underretningsplikt. Spesielt er det positivt at forordningen støtter opp under at personvern er mer enn konfidensialitet ved at «brudd på personopplysningssikkerheten» skal meldes inn til tilsynsmyndighetene. Det at den registrerte også skal underrettes, vil bidra til å styrke personvernet til den enkelte. Vi er imidlertid bekymret for at det kan oppstå ulik praksis for hva som menes med hhv. «risiko» og «høy risiko» i forordningens artikkel 33 og 34. Vi mener det er behov for veiledning for å sikre lik forståelse av artikkel 33 og 34 om melding eller underretning om brudd på personopplysningssikkerhet.

Vedlegg: Kommentarer til norsk oversettelse av EUs personvernforordning.

Vennlig hilsen

Christine Bergland e.f.
direktør

Birgitte Jensen Egset
avdelingsdirektør

Dokumentet er godkjent elektronisk

Kopi:
Helse- og omsorgsdepartementet (HOD)

September 2017

Kommentarer til norsk oversettelse av EUs nye personvernforordning

Direktoratet for e-helse har et internt prosjekt for å forberede innføring av EUs personvernforordning i mai 2018. I den forbindelse har vi gått gjennom den uoffisielle norske oversettelsen av EUs personvernforordning og sammenlignet den med den engelske versjonen. Direktoratet har følgende kommentarer til den norske oversettelsen av EUs personvernforordning:

A. Generelt

Ordet «safeguards» både i forordningens fortale og flere konkrete bestemmelse er oversatt til «garantier». En mer passende oversettelse kan være «sikringstiltak». «Garantier» forstås ofte som et løfte om rettigheter som skal innfris.

B. Kommentarer knyttet til enkeltbestemmelser

1. Artikkel 9 nr. 3

- Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

Oversettes til:

- Personopplysningene nevnt i nr. 1 kan behandles for formålene nevnt i nr. 2 bokstav h) dersom opplysningene behandles av en fagperson som har taushetsplikt i henhold til unionsretten eller medlemsstatenes nasjonale rett eller regler fastsatt av nasjonale vedkommende organer, eller av en annen person som også har taushetsplikt i henhold til unionsretten eller medlemsstatenes nasjonale rett eller regler fastsatt av nasjonale vedkommende organer.

Kommentarer:
Den norske oversettelsen mangler oversettelse av «or under the responsibility of».

2. Artikkel 12 nr. 1

- The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Oversettes til:

- Den behandlingsansvarlige skal treffe egnede tiltak for å framlegge for den registrerte informasjonen nevnt i artikkel 13 og 14 og all kommunikasjon i henhold til artikkel 15–22 og 34 om behandlingen på en kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk, især når det gjelder opplysninger som spesifikt er rettet mot et barn. Informasjonen skal gis skriftlig eller på en annen måte, herunder elektronisk dersom det er hensiktsmessig. På anmodning fra den registrerte kan informasjonen gis muntlig, forutsatt at den registrertes identitet bevises på andre måter.

Kommentarer:
"Any information" oversettes først til «informasjonen» og deretter til «opplysninger». Begrepet «informasjon» bør benyttes i begge setningene.

3. Artikkel 15 nr. 1

- The data subject shall have the right to obtain from the controller confirmation as to **whether or not** personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: …

Oversettes til:

- Den registrerte skal ha rett til å få den behandlingsansvarliges bekreftelse på om personopplysninger om vedkommende behandles, og, dersom dette er tilfellet, innsyn i personopplysningene og følgende informasjon: …

Kommentarer:
Den engelske teksten gir den registrerte en rettighet til å få en bekreftelse om personopplysninger om vedkommende behandles eller ikke behandles. Det norske teksten kan lett tolkes til bare å dekke situasjoner der den registrerte skal ha rett til å få den behandlingsansvarliges bekreftelse på at personopplysninger om vedkommende behandles.

4. Artikkel 15 nr. 4

- The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Oversettes til:

- Retten til å motta en kopi nevnt i nr. 3 skal ikke krenke andres rettigheter og friheter.

Kommentarer:
Forordningen skiller mellom «infridge» (krenke) og «adversely affect» (ha negativ innvirkning). Det er viktig at dette videreføres i den norske oversettelsen og at setningene oversettes riktig slik at meningsforskjellen mellom disse to begrepene kommer klart frem.
«Adversely affect» i denne konteksten bør oversettes til «å ha negativ innvirkning».

5. Artikkel 20 nr. 4

- The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Oversettes til:

- Rettigheten nevnt i nr. 1 skal ikke krenke andres rettigheter og friheter.

Kommentarer:
Se kommentar til Artikkel 15 nr. 4.

6. Fortalepunkt nr. 63

- That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software.

Oversettes til:

- Denne retten bør ikke krenke andres rettigheter eller friheter, herunder forretningshemmeligheter eller immaterialretten, særlig opphavsretten som programvaren er beskyttet av.

Kommentarer:
Se kommentar til Artikkel 15 nr. 4.

7. Artikkel 24 nr. 2

- Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

Oversettes til:

- Dersom det står i forhold til behandlingsaktivitetene, skal tiltakene nevnt i nr. 1 omfatte den behandlingsansvarliges iverksetting av retningslinjer for vern av personopplysninger.

Kommentarer:
Den norske oversettelsen fanger ikke opp nyansen som ligger i ordet «proportionate». Det er ikke nok at tiltak om iverksetting av retningslinjer står i forhold til behandlingsaktivitetene, da retningslinjer også må være et proporsjonalt tiltak. Det vil si at det må være forholdsmessig å iverksette de aktuelle retningslinjene på bakgrunn av behandlingsaktivitetenes natur.

8. Artikkel 29

- The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Oversettes til:

- Databehandleren og enhver person som handler for den behandlingsansvarlige eller databehandleren, og som har tilgang til personopplysninger, skal behandle nevnte opplysninger bare etter instruks fra den behandlingsansvarlige, med mindre det kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett.

Kommentarer:
Den norske oversettelse inneholder ordet "og" som ikke finnes i den engelske teksten. Det kan være gode grunner til at ordet «og» ikke finnes i den engelske teksten, og vi stiller spørsmål ved om tilføyelsen er bevisst.

9. Artikkel 32 nr. 1

- Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: …

Oversettes til:

- Idet det tas hensyn til det tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen, herunder blant annet, alt etter hva som er relevant, …

Kommentarer:
«As appropriate» i denne konteksten handler mer om hva som er passende. Noe kan være relevant men ikke passende.

10. Artikkel 40 nr. 2 bokstav k)

- out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

Oversettes til:

- utenrettslige prosesser og andre mekanismer for tvisteløsning mellom behandlingsansvarlige og databehandlere med hensyn til behandling, uten at det berører de registrertes rettigheter i henhold til artikkel 77 og 79.

Kommentarer:
Den norske oversettelsen inneholder feil i oversettelsen av «data subjects». Riktig oversettelse er «den registrerte».

11. Artikkel 89 nr. 1

- Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of

data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

Oversettes til:

- Behandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål skal omfattes av nødvendige garantier i samsvar med denne forordning for å sikre den registrertes rettigheter og friheter. Nevnte garantier skal sikre at det er innført tekniske og organisatoriske tiltak for særlig å sikre at prinsippet om dataminimering overholdes. Nevnte tiltak kan omfatte pseudonymisering, forutsatt at nevnte formål kan oppfylles på denne måten. Dersom nevnte tiltak kan oppfylles ved viderebehandling som ikke gjør det mulig eller ikke lenger gjør det mulig å identifisere de registrerte, skal formålene oppfylles på denne måten.

Kommentarer:
Den norske oversettelsen inneholder feil i oversettelse av «Where those purposes». Riktig oversettelse er «Dersom formålene».