Helsedirektoratet

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Deres ref.: 201201634 ES LLE/AHl/mk
Saksbehandler: CARIS
Vår ref.: 12/3717
Dato: 15.06.2012

Høringssvar - EU kommisjonens forslag til nye personvernregler

1. Innledning

Helsedirektoratet viser til Justis- og beredskapsdepartementets høring på EU-kommisjonens forslag til ny forordning om behandling av personopplysninger i EU/EØS. Forordningen skal erstatte gjeldende direktiv 95/46/EF. Departementet har bl.a. særskilt bedt om innspill på hvordan forslaget til forordning vil påvirke sektorlovgivningen. Direktoratet har derfor fokusert på innspill som gjelder direktoratets ansvarsområder, herunder forordningen regler sett i forhold til dagens lovgivning i helse- og omsorgssektoren.

2. Generelle kommentarer til forordningen

Direktoratet stiller seg positive til at flere av prinsippene fra gjeldende direktiv videreføres. Direktoratet stiller seg også positive til at det i flere av forordningens artikler fokuseres på økt bruk av elektroniske løsninger for kommunikasjon mellom databehandlingsansvarlig/behandlingsansvarlige og den registrerte, og ved overføring av personopplysninger fra et register til et annet. Direktoratet er opptatt av at det innføres sikre, elektroniske løsninger for å understøtte effektiv samhandling, ikke bare internt i helse- og omsorgssektoren men også mot tilgrensende sektorer. Samtidig ser direktoratet utfordringen ved å ta i bruk elektroniske løsninger uten at det tydeliggjøres hvilke formater, standarder etc. som skal benyttes. Dette vil kunne skape utfordringer f.eks. ved innføringen av elektroniske innsynsløsninger for borgerne.

Forordningen gir kommisjonen flere fullmakter til å fastsette detaljerte reguleringer innenfor flere områder. Et eksempel på denne adgangen er kommisjonens adgang til å spesifisere krav til informasjonssikkerhet i medhold av artikkel 30, tredje og fjerde ledd og adgangen til å gi utdypende krav til behandling av helseopplysninger i medhold av artikkel 81, tredje ledd. Direktoratet ser behovet for sikker kommunikasjon av personopplysninger over landegrensene, og ser viktigheten av det fastsettes hvilke formater, standarder etc. som benyttes. Uten felles standarder på tvers av landegrensene vil arbeidet med sikker elektronisk kommunikasjon av personopplysninger vanskeliggjøres.

Helsedirektoratet • Divisjon eHelse og IT
Avd. eHelse
Caroline Ringstad Schultz, tlf.: 24 16 36 28
Postboks 7000 St. Olavs plass, 0130 Oslo • Besøksadresse: Universitetsgata 2, Oslo • Tlf.: 810 20 050
Faks: 24 16 30 01 • Org. nr.: 983 544 622 • postmottak@helsedir.no • www.helsedirektoratet.no

3. Kommentarer til de enkelte bestemmelsen

Det foreslås flere nye definisjoner i artikkel 4. Definisjonen av "genetic data" er ny, og er så langt direktoratet kan vurdere i samsvar med gjeldende norsk rett.

Det er inntatt en definisjon av "biometric data". Direktoratet har ingen kommentarer tilknyttet definisjonen, men vil påpeke at biometrisk data i fremtiden kan være interessant å vurderes benyttet for autentisering.

Det er også angitt en definisjon av helseopplysninger, dvs. "data concerning health". Helseopplysninger er i forordningen definert som all informasjon relatert til et individs fysiske eller mentale helse, samt informasjon relatert til individets rett til helsetjenester. Direktoratet antar at dette innebærer at all kontakt med helsevesenet er å anse som helseopplysninger. Dette vil være i overensstemmelse med det norske regelverket på området slik vi praktiser det i dag.

Det er gitt en definisjon av samtykke i artikkel 4 nr. 8. Det stilles krav om at samtykke må være "explicit". Begrepet utdypes i fortalens punkt 25. Det oppstilles i forordningen et krav om en aktiv bekreftelse – enten ved en erklæring/uttalelse eller en aktiv handling av den registrerte. Dette innebærer at et stilltiende samtykke som rettslig grunnlag for behandling av personopplysninger ikke kan godtas. Dette er i overensstemmelse med samtykkekravet i helseregisterloven, hvor det stilles krav om utrykkelig samtykke for behandling av helseopplysninger.[1] Presiseringen vil derfor ikke ha konsekvenser for det norske regelverket. Endringen vil innebære at en løsning kun med reservasjonsrett som rettsgrunnlag for behandling av helseopplysninger ikke vil tifredsstille forordningens krav til samtykke.

Artikkel 7 er ny i forhold til gjeldende personverndirektiv. Her angis kravene til samtykke. Etter det direktoratet kan bedømme er dette i overensstemmelse med helseregisterlovens regler om samtykke. Samtykke skal imidlertid etter fjerde ledd ikke kunne benyttes som rettsgrunnlag for behandling av personopplysninger der det foreligger en "significant imbalance" mellom databehandlingsansvarlig og den registrerte. Etter vår mening er det sentralt at spesifiseringen i fortalens avsnitt 34 opprettholdes, slik at det offentliges behandling av personopplysninger om borgerne som regel ikke vil innebære at det er oppstått en "significant imbalance", da samtykke ofte benyttes som rettsgrunnlag for det offentliges behandling av helseopplysninger. Direktoratet mener i tillegg det kan presiseres enda tydeligere hva som ligger i uttrykket "significant imbalance" siden samtykke ofte vil være rettsgrunnlag for behandling av helseopplysninger bl.a. for å ivareta den registrertes personvern.

I forordningens artikkel 12 angis prosedyrer og mekanismer for den registrerte slik at vedkommende kan ivareta egne rettigheter. Etter første ledd skal den registrerte som ønsker å ivareta sine rettigheter, der personopplysningene er behandlet elektronisk, kunne sende en henvendelse til den databehandlingsansvarlige/behandlingsansvarlige elektronisk. Etter andre ledd skal den registrerte som ber om innsyn i egne opplysninger elektronisk også motta opplysningene elektronisk med mindre vedkommende ber om utlevering på papir.

[1] Lov om helseregistre og behandling av helseopplysninger (helseregisterloven), Lov-2001-05-18-24.

Det er ikke nærmere beskrevet hva som ligger i "automated means" (elektronisk behandling) og hvilke format/standarder eventuelle utleveringer skal skje på. I den norske helse- og omsorgssektoren foregår i økende grad elektronisk behandling av helseopplysninger. Det vil derfor være behov for å fokusere på standarder for å kunne ivareta elektroniske forespørsler samt utlevere opplysninger på en sikker og effektiv måte til borgerne i tråd med bestemmelsen. Forordningens krav til elektronisk behandling f.eks. av innsynsbegjæringer over landegrensene kan dermed være vanskelig å fullt ut etterleves uten definerte standarder på området.

Artikkel 17 inneholder bestemmelser om retten til å bli glemt, herunder retten til å få slettet lagrede opplysninger om seg selv. I artikkelens første ledd oppstilles en rett for den enkelte til å kreve at databehandlingsansvarlig sletter opplysninger om vedkommende og at han avstår fra og spre opplysningene videre, dersom ett av følgende vilkår er tilstede:

a) dersom det ikke lenger er behov for opplysningene til det formål de ble samlet inn for.

b) samtykke trekkes tilbake i situasjoner der behandling av helseopplysninger til det/de aktuelle formål er basert på samtykke fra vedkommende, eller samtykke er gått ut på dato, og det ikke lenger foreligger et gyldig samtykke.

c) rett til å motsette seg behandlingen etter artikkel 19 – right to object

d) behandling av opplysninger er i strid med forordningen

Det er et spørsmål om forordingens bestemmelse gir den enkelte en mer omfattende rett til å få slettet opplysninger enn det som kan kreves slettes med hjemmel i helsepersonelloven og helseregisterloven.[2]

Når det gjelder opplysninger som er innhentet i forbindelse med helsehjelp fremgår det av helsepersonelloven § 43 når opplysninger kan slettes. Det fremgår her at opplysninger som er registrert i forbindelse med helsehjelp skal slettes dersom dette er ubetenkelig ut fra allmenne hensyn, ikke strider mot bestemmelser i eller i medhold av arkivloven §§ 9 eller 18 og:

1. opplysningene er feilaktige eller misvisende og føles belastende for den de gjelder eller
2. opplysningene åpenbart ikke er nødvendige for å gi pasienten helsehjelp

Når det gjelder behandling av helseopplysninger som er samlet inn til annet formål enn helsehjelp, for eksempel til forskning, og som ikke skal registreres i pasientjournal i medhold av helsepersonelloven §§ 39 og 40, er sletteretten regulert i annet regelverk. Det følger av helseregisterloven § 28 at den registrerte kan kreve at helseopplysninger slettes, dersom behandling av opplysningene føles sterkt belastende for den registrerte og det ikke finnes sterke allmenne hensyn som tilsier at opplysningene behandles.

Dersom behandling av helseopplysninger er basert på samtykke, følger det av kravene til et gyldig samtykke at dette når som helst kan trekkes tilbake.

---

[2] Lov om helsepersonell m.v. (helsepersonelloven), LOV-1999-07-02-64.

Etter det direktoratet kan se går ikke forordningen lenger i å åpne for sletting enn hva som er tilfelle i norsk rett, og vi antar derfor at sletteretten etter forordningen er sammenfallende med helsepersonellovens og helseregisterlovens bestemmelser.

Det følger videre av artikkelens andre ledd at dersom databehandlingsansvarlig har publisert ("made public") opplysninger som vedkommende har krav på å få slettet etter første ledd, så skal databehandlingsansvarlig ta rimelige skritt, herunder tekniske tiltak med tanke på dataene som vedkommende er ansvarlig for publiseringen av, for å informere tredjeparter som behandler slike data om at den registrerte krever at de sletter enhver gjengivelse av de aktuelle personopplysninger.

Det er her et spørsmål om hva som menes med å publisere opplysninger.
I punkt 54 i fortalen vises det til at det her er snakk om online publisering.
Alle som behandler helseopplysninger i medhold av helsepersonelloven og helseregisterloven vil være underlagt helsepersonellovens og forvaltningslovens taushetspliktsregler, jf. helseregisterloven § 15, jf. helsepersonelloven § 21. Dette innebærer at det ikke kan utleveres/videreformidles opplysninger uten at det foreligger et unntak fra taushetsplikten. Vi antar at det å utlevere helseopplysninger i tråd med helselovgivningens utleveringsbestemmelser (bestemmelser som innebærer unntak fra taushetsplikten), eks. når NPR med hjemmel i forskrift utleverer data til forskning, ikke er å anse som å " make the personal data public". Direktoratet stiller imidlertid spørsmål ved om elektroniske innsynsløsninger for den registrerte selv, der vedkommende på autentisere seg for å få tilgang til opplysningene, innebærer at opplysningene er "made public". Direktoratet tolker bestemmelsen slik at slike tilfeller ikke er ment å falle inn under bestemmelsen, og mener dette også er det mest hensiktsmessige da slike løsninger er basert på lov eller den registrertes samtykke, og utvekslingen av opplysninger til 3 part er lovregulert.

Det følger av artikkel 17, tredje ledd, at selv om vilkårene for å slette i medhold av første ledd er oppfylt, så skal det allikevel være tillatt å beholde dataene bl.a. av hensyn til allmennhetens interesse på område folkehelse, jf. artikkel 81. Dette innebærer at samfunnets interesse i å beholde dataene i disse tilfellene vil gå foran den enkeltes rett til å slette. Etter det vi kan se er dette i overensstemmelse med norsk rett. Det følger av helseregisterloven § 28 at dersom det foreligger sterke allmenne hensyn som tilsier at opplysningene behandles, så vil dette gå foran den enkeltes rett til å slette.

Artikkel 18 gir borgerne rett til å motta en elektronisk versjon av opplysningene (der opplysningene behandles elektronisk) på en strukturert måte og i et vanlig format. I tillegg skal den registrerte kunne overføre opplysningene elektronisk i et vanlig format til et annet system, men kun der vedkommende selv har gitt den behandlingsansvarlige/databehandlingsansvarlige opplysningene og behandlingen er basert på samtykke/kontrakt. Bestemmelsen skaper en utfordring i forhold til hva som er "electronic format which is commonly used". Det kan stilles spørsmål ved om begrepet "electronic format" viser til maskinlesbart eller menneskelesbart format. Det bør derfor tydeliggjøres hvilket nivå man ønsker å legge seg på, slik at kommisjonen kan presisere hvilken struktur eller semantikk som bør benyttes ved presentasjon av informasjon. Uten en nærmere klargjøring av hvilke standarder som skal benyttes vil det være vanskelig å oppfylle bestemmelsen krav.

Artikkel 24 omhandler tilfellet der en behandling av personopplysninger har flere databehandlingsansvarlige/behandlingsansvarlige. Direktoratet tolker bestemmelsen slik at den pålegger de databehandlingsansvarlige/behandlingsansvarlige ved delt ansvar å avtale seg imellom hvilke oppgaver som skal utføres av den enkelte virksomhet. Direktoratet ser det som viktig at det avtales tydelige hvilke oppgaver den enkelte virksomhet skal utøve. I tillegg er det positivt at det oppstilles krav om solidaransvar for virksomheter som har delt databehandlingsansvar jf. artikkel 77, andre ledd. Uten krav om solidaransvar kan det være vanskelig for den registrerte å vite overfor hvem vedkommende kan kreve sine rettigheter etter forordningen oppfylt.

Artikkel 35 oppstiller krav om personvernombud for offentlige virksomheter, virksomheter med mer enn 250 ansatte, og virksomheter som har regelmessig og systematisk monitorering av personer som sin hovedbeskjeftigelse. Dette vil påvirke flere virksomheter i helse- og omsorgssektoren som i dag ikke deltar i den frivillige norske ordningen. Siden mange av disse virksomhetene er små og ikke nødvendigvis innehar nødvendige ressurser for å ivareta oppgaven, er det er viktig at adgangen for flere virksomheter til å benytte samme personvernombud opprettholdes, og at vedkommende både kan være ansatt i eller utføre oppgaven på bakgrunn av serviceavtale med virksomheten.

I Artikkel 38 omtales ønske om å bidra til utvikling av "Code of Conducts". Norge har på helseområdet utviklet Norm for informasjonssikkerhet for helse-, omsorgs-, og sosialsektoren (Normen).[3] Normen inneholder lovverkets krav til informasjonssikkerhet, men stiller også på noen områder opp strengere krav enn hva som er beskrevet i lovverket. Den blir bindende for virksomheter som tilknyttes helsenettet, ved at virksomhetene i tilknytningsavtalen skriver under på at de skal følge Normen.

Normen er utarbeidet av representanter for helse-, omsorgs- og sosialsektoren og forvaltes av en Styringsgruppe bestående av sektorens representanter. Helsedirektoratet leder styringsgruppen og innehar sekretariatsfunksjon. Direktoratet har god erfaring med bransjenorm som et virkemiddel for å heve kompetansen og etterlevelsen av krav til informasjonssikkerhet i helsesektoren i Norge. Direktoratet er derfor positive til at arbeid med bransjenormer skal støttes i fremtiden.

I artikkel 81 gis det regler for behandling av helseopplysninger. Bestemmelsen oppstiller vilkår for behandling av helseopplysninger, og gjelder etter direktoratets oppfattelse all behandling av helseopplysninger, uavhengig av rettslige grunnlaget for behandling. Bestemmelsen gjelder derfor også ved behandling av helseopplysninger der samtykke er rettslig grunnlag. Etter det vi kan se er vilkårene i bestemmelsen i overensstemmelse med gjeldende norsk rett.

Vennlig hilsen

Norunn Elin Saure e.f.
avdelingsdirektør

Caroline Ringstad Schultz
rådgiver

Dokumentet er godkjent elektronisk

[3] www.normen.no