Norsk helsenett

En databehandler, flere databehandlere, alle databehandlerne – en juridisk oppfriskning

Ståle Norum Engen
jurist

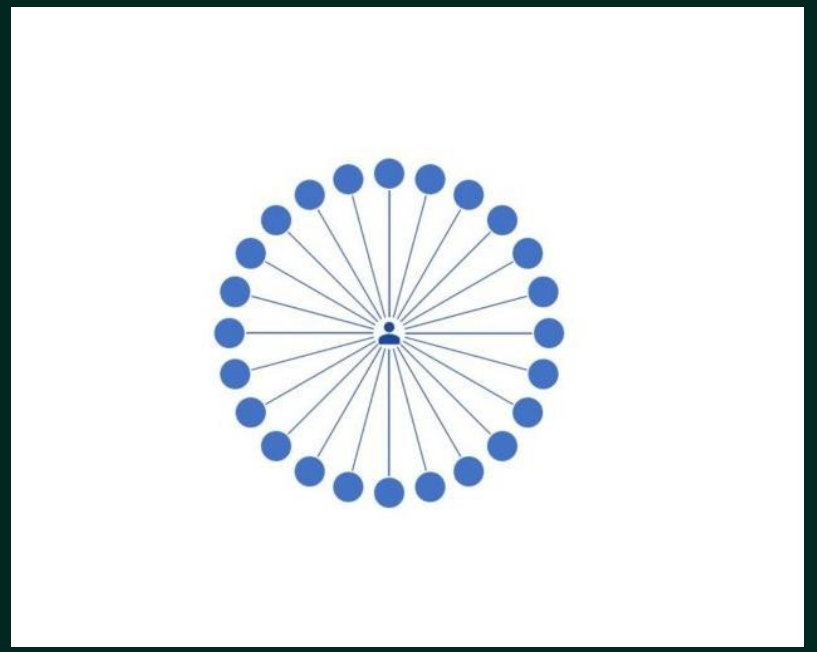
November 2023

Normkonferansen

Personopplysninger

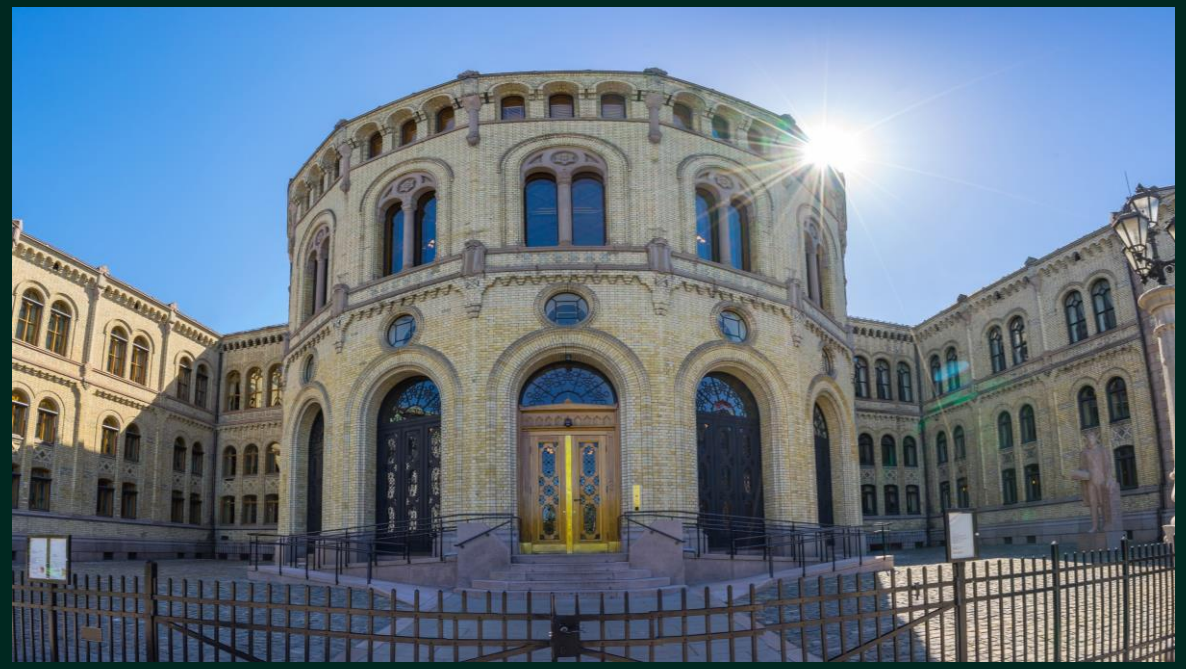
- Personvernforordningen (GDPR) fra EU av 2016
  - Gjort til norsk lov ved Personopplysningsloven av 2018

- Hva er en personopplysning?
  - GDPR art. 4 nr. 1:
  - «I denne forordning menes med «personopplysning» 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, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet»



Personvernprinsipper

- Behandlingen må være lovlig → ha behandlingsgrunnlag
- Behandlingen må skje rettferdig
- Behandlingen skal være gjennomsiktig
- Formålsbegrensning
- Dataminimering
- Riktighet
- Lagringsbegrensning
- Integritet og konfidensialitet
- Ansvarlighet



De registrertes rettigheter og friheter

- rett til informasjon
- rett til informasjon
- rett til innsyn
- rett til å få rettet uriktige personopplysninger om seg selv
- rett til sletting / å bli glemt
- rett til begrensning av behandling
- rett til dataportabilitet
- rett til å protestere
- rett til ikke å være gjenstand for automatiserte individuelle avgjørelser

➢ Artikler 13 – 22 i GDPR

Behandlingsansvarlig og databehandler

- Behandlingsansvarlig → Dataansvarlig
  - «en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes»
  - Kalt dataansvarlig i helsesektoren:
    Se bl.a. Pasientjournalloven § 2 bokstav e) og Helseregisterloven § 2 bokstav d)

- Databehandler
  - «en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige»

  - GDPR art. 4 nr. 7 og 8 + kapittel IV (art. 24-43)

Ansvar

Dataansvarlig

- Overordnet ansvar for etterlevelse av GDPR
- Sørge for behandlingsgrunnlag
- Ansvarlig for overholdelse av de registrertes rettigheter og friheter
- Overordnet ansvarlig for tiltak
- Forsvarlig valg av databehandler

Databehandler

- Behandler på vegne av
- Behandler på instruks
- Gi tilstrekkelige garantier til dataansvarlig
- Treffe nødvendige sikkerhetstiltak
- Bistå dataansvarlig
- Har en del selvstendig ansvar som vi skal komme nærmere tilbake til…

Foreligger det et databehandleroppdrag?

- Behandles det personopplysninger på andres vegne?
  - Skal leverandøren behandle personopplysninger for den dataansvarlige?
- Går oppdraget ut på å behandle personopplysninger?
  - Er formålet helt eller delvis at det skal behandles personopplysninger?
- Det foreligger ikke alltid en databehandlerrelasjon selv om man må utlevere personopplysninger for å motta en tjeneste.
  - Gis det imidlertid tilgang til personopplysninger i stor eller systematisk grad, vil oppdraget kunne sies å delvis bestå i å behandle personopplysninger, selv om ikke dette er hovedoppdraget.
- Er det en part som bestemmer formålet med behandlingen?
- Hvem bestemmer i hovedsak hvilke midler (tekniske løsninger eller organisatoriske beslutninger) som skal brukes?

Datatilsynet:

«Hva som er bestemt ved avtale mellom partene kan også ha betydning i vurderingen. Det forutsetter at det ikke er tvil om at avtalen reflekterer de faktiske forholdene, og hvem som faktisk bestemmer. Man kan altså ikke avtale at en virksomhet er behandlingsansvarlig dersom virksomheten reelt sett er en databehandler, og omvendt. Med andre ord kan du ikke avtale deg bort fra ansvaret du har etter personvernregelverket.»

Databehandleren

- Skal kun behandle personopplysninger på vegne av den dataansvarlige
  - Samt forholde seg til lovpålagte plikter i annet regelverk…
- Behandler alltid personopplysninger etter dokumenterte instrukser fra en dataansvarlig, og kan derfor ikke bestemme formål og andre avgjørende elementer ved behandlingen
  - Kan også instrueres ved dataansvarliges egen konfigurering av en løsning / tjeneste
- Skal gi dataansvarlig tilstrekkelige garantier
- Må som regel utpeke et personvernombud
- Kan bidra til å ivareta tillit hos kunder / de registrerte – ved å demonstrere kontroll og kunnskap om regelverket

Databehandler har mange plikter etter GDPR

- Overholdelse av GDPR – handlinger eller unnlatelser som kan trigge sanksjoner
  - Gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller GDPR
- Hjelpe til å etablere en databehandleravtale som oppfyller GDPR
- Sikkerhet
  - GDPR forplikter databehandlere til å ta passende sikkerhetstiltak for å beskytte personopplysningene de behandler.
  - Sikre konfidensialitet / taushetsplikt
  - Varsle den dataansvarlige om avvik
- Bistå den dataansvarlige
  - Med å oppfylle krav til innsyn fra den registrerte
  - Med å svare ut henvendelser fra de registrerte som ønsker å utøve sine rettigheter (retting, sletting, informasjon, protestere osv.)
  - Med informasjon til tilsynsmyndigheten eller den registrerte, DPIA og forhåndsdrøftinger
- Muliggjøre og bidra til revisjoner og inspeksjoner
- Føre protokoll
- Ikke engasjere underleverandører uten særlig eller generell skriftlig tillatelse
- Ikke overføre personopplysninger til en tredjestat uten instruksjoner eller rettslig krav

Databehandleravtale

Datatilsynet:

«I artikkel 28 i personvernforordningen finner man kravene til innholdet i en databehandleravtale. Det er imidlertid ikke noe i veien for at inneholder flere vilkår enn det som følger av loven, for eksempel dersom den behandlingsansvarlige ønsker å gi databehandleren særlige forpliktelser. Dette er opp til den behandlingsansvarlige å vurdere. Det er også opp til den behandlingsansvarlige å vurdere om databehandleravtalen skal inneholde Datatilsynets anbefalinger utover kravene i loven.»

Databehandleravtale

- Må beskrive selve behandlingen
  - Avtalens tema og behandlingens art, formål og varighet
  - Kategorier av registrerte som omfattes, og hva slags personopplysninger som behandles
- Skal ivareta den dataansvarliges plikter og rettigheter
  - ansvarlig for at personopplysninger blir behandlet i samsvar med personvernforordningen og personopplysningsloven
  - har både en rett og en forpliktelse til å bestemme hvilke formål, og hvilke hjelpemidler som kan brukes i behandlingen
  - skal gi databehandleren dokumenterte instrukser for hvordan personopplysninger skal behandles
  - rett til å si opp avtalen dersom databehandleren ikke lenger oppfyller lovens / forordningens krav

Databehandleravtale

- Skal beskrive nærmere databehandlerens forpliktelser
  - Tilgjengeliggjøring av informasjon for den dataansvarlige
  - Bare behandle personopplysninger etter skriftlig instruks fra den behandlingsansvarlige
  - Autoriserte personer skal behandle personopplysningene fortrolig
  - Plikt til å ha tilfredsstillende sikkerhetstiltak
  - Underretning om brudd på personopplysningssikkerheten
  - Bruk av annen databehandler (underleverandør)
  - Overføring til tredjeland
  - Bistand til å svare på anmodninger som gjelder de registrertes rettigheter
  - Annen bistand til den dataansvarlige
  - Revisjon og inspeksjon
  - Sletting og returnering av opplysninger
  - Avslutning av avtalen

Standardavtaler / sterke databehandlere

Datatilsynet:

«Mange databehandlere tilbyr spesifikke tjenester som innebærer behandling av personopplysninger og har derfor «standard databehandleravtaler». Ved bruk av slike standardavtaler kan man kanskje få inntrykk av at det er databehandleren som bestemmer fordi avtalen inneholder vilkår for hvordan databehandleren behandler personopplysninger. Ansvaret for at vilkårene etterlever personvernregelverket ligger likevel hos den behandlingsansvarlige. Den behandlingsansvarlige har derfor ansvar for å undersøke at standardavtalen etterlever regelverket.»

Oppfølging av databehandleravtaler

- Innkjøp og databehandleravtaler
- Avtalerevisjon / oppfølging
- Internkontroll (i praksis GDPR art. 24)
- Her er protokoller nyttige verktøy
- Tiltak skal gjennomgås på nytt og oppdateres ved behov, jf. GDPR art. 24
- DPIAer må gjennomgås og endres ved behov, jf. GDPR art. 35 nr. 11
- Prosess for regelmessig testing, analysering og vurdering av hvor effektive tekniske og organisatoriske sikkerhetstiltak er, jf. GDPR art. 32 nr. 1 bokstav d)

Sanksjoner

- Dataansvarlig er i utgangspunktet alltid ansvarlig
  - Regress mot databehandler som har brutt avtale / instruks
  - Avtalte misligholdsbeføyelser og erstatningsbestemmelser i den overordnede kontrakten / tjenesteavtalen mellom dataansvarlig og databehandler.
- Erstatningsansvar:
  - «En databehandler skal være ansvarlig for en skade forårsaket av behandling bare dersom vedkommende ikke har oppfylt forpliktelsene i denne forordning som er særlig rettet mot databehandlere, eller dersom vedkommende har opptrådt utenfor eller i strid med databehandlerens lovlige instrukser.» GDPR art. 82 nr. 2.
- Overtredelsesgebyr:
  - Kan også ilegges databehandler. GDPR art. 83
  - Kan særlig være aktuelt om databehandler gjør seg til dataansvarlig ved sine handlinger.

Norsk helsenett

Vi knytter Helse-Norge sammen