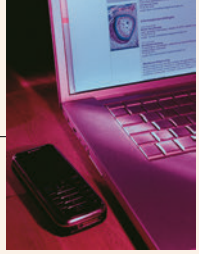

# Ny personvernforordning – hva betyr den for din tannlegevirksomhet?

I den senere tid har det vært et økt oppmerksomhet rundt hvordan bedrifter skal forberede seg på ny lovgivning innen personvernområdet.

Personvernforordningen GDPR (General Data Protection Regulation) trer i kraft 25. mai 2018, og Justis- og beredskapsdepartementet sendte den 6. juli 201 forslag til ny personopplysningslov ut på høring, med høringsfrist 16. oktober. Lovforslaget omhandler gjennomføringen av EUs personvernforordning. Det tas sikte på at ny personopplysningslov skal tre i kraft samtidig med forordningen.

## Bakgrunn

Samfunnet har i de senere år vært i en radikal digital endring. Med økt bruk av digitale medier registreres og brukes personopplysninger nå nærmest overalt. Den digitale utviklingen har gått fort og det eksisterende lovverket er ikke tilpasset dagens hverdag. Med dette som bakgrunn har EU gått inn for å styrke privatpersoners rettigheter og samtidig skjerpe bedriftenes forpliktelser. Forordningen innebærer de største endringene i personvernlovgivningen i EU på 23 år. Gjennomføringen medfører at det må foretas betydelige endringer i hvordan bedrifter behandler personopplysninger.

Forordningen innebærer en full harmonisering av personvernregelverket i EU/EØS. I utgangspunktet vil det ikke være adgang til å fravike reglene og heller ikke til å supplere reglene i forordningen. Forordningen åpner imidlertid for at det i enkelte tilfeller kan gis nasjonale regler. Praksis fra EU på forordningens område vil ha stor betydning for hvordan forordningen skal tolkes og forstås også i Norge.

Norske myndigheter har foreslått å innføre GDPR ved inkorporasjon, hvilket innebærer at forordningen vil gjelde som norsk rett slik som den er. Der hvor forordningen gir anledning for nasjonale tilpasninger har departementet foreslått en videreføring av gjeldende regler.

## Endringer fra dagens situasjon

Forordningen medfører omfattende endringer i forhold til dagens regelverk. Det vil imidlertid bli for omfattende å gå inn på hver enkelt endring som vil komme som følge av forordningen. Det er derfor valgt å gå nærmere inn på de endringer som anses som mest relevante og sentrale.

## Personvernrådgiver

Forordningens regler vedrørende personvernrådgiver innebærer en betydelig utvidelse i forhold til gjeldende norsk rett. Alle offentlige myndigheter samt enkelte private behandlingsansvarlige blir pålagt å opprette personvernrådgiver. Hvem som må opprette personvernrådgiver følger av forordningens artikkel 37. Når det gjelder privat sektor er det bedrifter som har som hovedvirksomhet å regelmessig og systematisk monitorere personer, og som behandler sensitive personopplysninger, eller opplysninger om straffbare forhold i stor skala som er pliktige til å opprette personvernrådgiver.

I ovennevnte ligger det at det blant annet ikke er klarlagt hva som ligger i begrepet «stor skala». Dette medfører en usikkerhet for når en bedrift må opprette personvernrådgiver. Datatilsynet har søkt å presisere hva som skal forstås med «stor skala» og nevner for eksempel at fastleger og advokater som kun behandler opplysninger for et begrenset antall pasienter eller klienter er eksempel på aktører som ikke behandler personopplysninger i «stor skala».

Da det på nåværende tidspunkt er usikkert hva som helt konkret skal forstås med «stor skala», er det ikke mulig å si hvilken betydning dette får for den enkelte tannlegevirksomhet. Datatilsynet vil forhåpentligvis bli mer konkrete innen regelverket trer i kraft.

Med mindre det er helt opplagt at bedriften ikke er pålagt å ha personvernrådgiver, råder Datatilsynet alle bedrifter til å dokumentere de vurderinger som er foretatt dersom bedriften velger å ikke opprette personvernrådgiver.

## Varsling

Etter gjeldende regelverk stilles det krav til at eventuelle avvik eller sikkerhetsbrudd skal håndteres internt i virksomheten. Datatilsynet skal varsles dersom det har vært «uautorisert utlevering av personopplysninger som krever konfidensialitet».

Ved ikrafttredelsen av GDPR skjerpes kravene til når avvik skal rapporteres til Datatilsynet. Som den store hovedregel skal alle avvik som skyldes brudd på datasikkerhet meldes inn til Datatilsynet. Unntak gjelder dersom det er usannsynlig at avviket medfører en risiko for enkeltpersoners rettigheter eller personvern. Etter de nye reglene vil den behandlingsansvarlige bli ansvarlig for å varsle Datatilsynet «uten ugrunnet opphold» og senest 72 timer etter å ha blitt kjent med et sikkerhetsbrudd. Det stilles også krav til at databehandlere umiddelbart skal varsle behandlingsansvarlige dersom de oppdager avvik.

## Retten til å bli glemt

Ved forordningen får den registrerte en tydeligere rett til å kreve sletting av egne personopplysninger. Retten til å kreve sletting kalles retten til å bli glemt og er regulert i forordningens artikkel 17.

Den registrerte kan etter forordningen blant annet kreve at opplysningene om ham eller henne slettes når opplys-

ningene ikke lenger er nødvendige for å oppnå formålet med behandlingen, samtykket til behandlingen er trukket tilbake og det ikke finnes et annet rettslig grunnlag for behandlingen, den registrerte har fremsatt en berettiget innsigelse og hvor personopplysninger er blitt behandlet på en måte som ikke er lovlig. Retten til å bli glemt, «sletteplikten», gjelder imidlertid ikke dersom opplysningene er nødvendig for at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse, den er nødvendig for allmenhetens interesse knyttet til folkehelse og videre når den er nødvendig for arkivformål i allmennhetens interesse.

**Dataportabilitet**

Dataportabilitet er en ny rettighet som går ut på at den registrerte vil kunne kreve å få sine personopplysninger overført fra en virksomhet til en annen. Selve formålet med dataportabilitet er å gi den registrerte kontroll over sine egne opplysninger. Retten til dataportabilitet gjelder imidlertid kun egne opplysninger som den registrerte selv har gitt til den behandlingsansvarlige. Dataportabilitet er regulert i GDPR artikkel 20.

Dataportabilitet kan skje ved at den registrerte får utlevert personopplysninger i et strukturert, alminnelig anvendt og maskinlesbart format slik at disse kan overføres til en annen behandlingsansvarlig. I den grad det er teknisk mulig har den registrerte rett til å få personopplysningene overført direkte fra en behandlingsansvarlig til en annen.

**Bransjenorm**

Forordningen oppfordrer til at virksomheter innen samme sektor går sammen og utarbeider bransjenormer. Dette vil si at det utvikles retningslinjer for hvordan en sektor eller bransje skal sikre at den behandler personopplysninger på en riktig og god måte. Slike bransjenormer skal etter de nye reglene godkjennes av Datatilsynet.

Innen helsesektoren har vi «Norm for informasjonssikkerhet helse og omsorgstjenesten» (Normen) som er et omforent sett av krav til informasjonssikkerhet basert på dagens lovverk. Normen er utarbeidet av representanter for helse-, omsorgs- og sosialsektoren, herunder Tannlegeforeningen. Hensikten med normen er at den skal bidra til å etablere mekanismer hvor de forskjellige virksomhetene kan ha gjensidig tillit til at behandling av helse- og personopplysninger gjennomføres forsvarlig. GDPR vil føre til innholdsendringer samt endringer i «organiseringen» av Normen. Det er nå ikke klart hva disse endringene vil gå ut på.

**Overtredelsesgebyr**

Etter gjeldende rett kan Datatilsynet ilegge et overtredelsesgebyr for overtredelser av personopplysningsloven eller forskriften med et beløp på inntil ti ganger folketrygdens grunnbeløp, dvs. inntil NOK 936 340 (1 G = NOK 93 634 pr 1.5.2017). Ved utmålingen av overtredelsesgebyret skal det legges vekt på overtredelsens alvor, graden av skyld, om overtredelsen kunne vært forebygget, om det foreligger gjentagelse etc.

I henhold til GDPR artikkel 83 skal de nasjonale tilsynsmyndigheter sikre at overtredelsesgebyr i den enkelte sak er virkningsfulle, står i forhold til overtredelsen samt at det virker avskrekkende. GDPR åpner for at Datatilsynet kan ilegge et overtredelsesgebyr på opptil 20 millioner euro eller hvis det er gjelder foretak, 4 % av den globale årsomsetningen i forutgående regnskapsår hvis denne er høyere. Dette medfører at maksimumsbeløpet på overtredelsesgebyret økes betraktelig. Overtredelsesgebyret vil være å anse som straff etter EMK, og vil dermed omfattes av de rettssikkerhetsgarantiene konvensjonen fastsetter.

**Oppsummert**

Inkorporeringen og ikrafttredelsen av GDPR medfører at privatpersoners rettigheter styrkes betraktelig, og bedrifters forpliktelser skjerpes tilsvarende. Det er på nåværende tidspunkt uklart hvordan enkelte deler av forordningen skal tolkes og forstås, hvilket medfører en usikkerhet sett i forhold til hvordan den enkelte bedrift skal forholde seg.

Det er imidlertid viktig å sikre seg at bedriften per i dag følger gjeldende regelverk og allerede nå innehar gode rutiner for håndtering av personopplysninger. Om dette er på plass er en kommet et godt stykke på vei. Hvordan de endelige reglene blir er imidlertid ikke mulig å si helt sikkert før ny personopplysningslov er vedtatt og Datatilsynet mest sannsynlig kommer med sine fortolkninger av tvilstilfeller.

NTFs sekretariat følger med på prosessen med tanke på betydningen for våre medlemmer, og vi vil komme med mer informasjon når dette foreligger. Ved eventuelle spørsmål kan sekretariatet kontaktes. Ellers anbefaler vi at det følges med på Datatilsynet sine sider www.datatilsynet.no. På Datatilsynet sine sider ligger også en foreløpig norsk oversettelse av forordningen, se: https://www.datatilsynet.no/globalassets/global/regelverk-skjema/forordningen/uoffisiell-norsk-oversettelse-av-personvernforordningen.pdf.

*Ann-Britt Rognes*
*Advokat i NTF*