Den norske tannlegeforening

Hvorfor trenger vi å inngå ny databehandleravtale?

Når den nye personopplysningsloven og GDPR trer i kraft blir kravene til databehandleravtalene langt mer omfattende enn etter dagens lovverk. Det er viktig at databehandleravtalene tilfredsstiller de nye kravene.

Når personopplysninger behandles på vegne av andre, skal det foreligge en avtale som regulerer behandlingen. Denne avtalen kan enten være en selvstendig kontrakt eller en del av en kontrakt som også regulerer andre ytelser. Det er den som er ansvarlig for behandling av personopplysningene, den *behandlingsansvarlige*, som også er ansvarlig for at det inngås databehandleravtale. Den som behandler opplysninger på vegne av den behandlingsansvarlige, *databehandleren*, har ikke noe direkte ansvar for at databehandleravtale inngås.

Etter dagens personopplysningslov er det kun to eksplisitte krav til databehandleravtaler: Databehandleravtalen skal regulere hvordan databehandleren skal behandle personopplysningene på vegne av den behandlingsansvarlige, og databehandlerens plikt til å sørge for informasjonssikkerhetstiltak skal reguleres, jf. personopplysningsloven § 15.

De nye reglene medfører som nevnt at det blir flere og klarere krav til innholdet i databehandleravtalen. Kravene følger spesielt av artikkel 28 i GDPR, som blant annet sier at databehandleravtalen skal inneholde angivelse eller beskrivelse av:

- ***hensikten*** med behandlingen
- ***varigheten*** av behandlingen
- behandlingens ***formål og art***
- ***typen personopplysninger og kategorier av registrerte*** som skal behandles
- den ***behandlingsansvarliges rettigheter og plikter***

I tillegg skal databehandleren pålegges spesifikke plikter som at databehandleren skal:

- kun behandle personopplysningene på ***instruks*** fra den behandlingsansvarlige (som kan dokumenteres i ettertid)
- ikke overføre personopplysninger til land utenfor EU/EØS (tredjeland) uten etter instruksjon fra den behandlingsansvarlige
- sikre at personer som er autorisert til å behandle personopplysningene **har *forpliktet seg til å behandle opplysningene fortrolig* eller *er underlagt en egnet lovfestet taushetsplikt***
- treffe alle tiltak som er nødvendig for ***sikkerhet ved behandlingen, og gjennomføring av tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå*** som tar hensyn til relevant risiko ved behandlingen etter artikkel 32 i GDPR
- kun ***engasjere en annen databehandle***r («underdatabehandler») dersom det på forhånd er innhentet særlig eller generell skriftlig tillatelse til dette behandlingsansvarlig. Er det gitt en generell tillatelse, skal databehandleren underrette den behandlingsansvarlige om eventuelle planer om å benytte andre databehandlere eller skifte ut databehandlere, og dermed gi den behandlingsansvarlige muligheten til å motsette seg slike endringer. Engasjeres det underdatabehandler, skal denne pålegges de samme forpliktelsene til vern av

personopplysninger som er fastsatt i databehandleravtalen. Hvis underdatabehandler ikke oppfyller forpliktelsene sine, skal databehandleren ha fullt ansvar for at underdatabehandleren oppfyller sine forpliktelser overfor den behandlingsansvarlige

- etterkomme pålegg fra den behandlingsansvarlige om **å *slette eller tilbakelevere alle personopplysninger*** (inkludert kopier) etter at tjenestene knyttet til behandlingen er avsluttet, med mindre det foreligger lovkrav til at opplysningene skal fortsatt lagres
- gjøre ***tilgjengelig all informasjon som er nødvendig for å påvise at forpliktelsene ovenfor er oppfylt*** for den behandlingsansvarlige, samt muliggjøre og bidra til revisjoner og inspeksjoner som gjennomføres av den behandlingsansvarlige eller annen på dennes vegne
- omgående ***underrette den behandlingsansvarlige*** dersom en instruks fra den behandlingsansvarlige er i strid med GDPR eller andre bestemmelser om vern av personopplysninger, som personopplysningsloven.

Databehandleren skal bistå den behandlingsansvarlige med oppfyllelse av plikter, som skal reguleres i databehandleravtalen. Dette omfatter å bistå den behandlingsansvarlige med å:

- oppfylle pliktene til å ***svare på anmodninger*** som de registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i kapittel III i GDPR hensyntatt til behandlingens art og i den grad det er mulig ved hjelp av egnede tekniske og organisatoriske tiltak
- ***sikre overholdelse av forpliktelser*** etter artikkel 32–36, som er krav til sikkerhet ved behandlingen, melding til tilsynsmyndigheten (Datatilsynet) og eventuelt de registrerte om brudd på personopplysningssikkerheten, vurdering av personvernkonsekvenser (såkalte DPIAs) og ved forhåndsdrøftinger med Datatilsynet før behandling med høy risiko.

Etter GDPR stilles det ikke krav til at databehandleravtalen regulerer andre plikter som tilligger databehandleren, men det vil klart være en fordel at avtalen også inkluderer oppgaver og plikter som databehandleren har etter andre deler av GDPR. Dette vil være forhold som at Databehandleren skal *overholde godkjente atferdsnormer* etter artikkel 40 eller *overholde en godkjent sertifiseringsmekanisme* som nevnt i artikkel 42.

Visse databehandlere har plikt til å *føre skriftlig protokoll over alle kategorier av behandlingsaktiviteter* som er utført på vegne av en behandlingsansvarlig. Dette gjelder kun selskap/organisasjoner med flere enn 250 ansatte, med mindre behandlingen trolig vil medføre en risiko for de registrertes rettigheter og friheter, behandlingen ikke skjer leilighetsvis eller omfatter særlige kategorier av opplysninger (sensitive personopplysninger) eller personopplysninger om straffedommer og straffbare forhold. Dersom det skal føres slik protokoll, bør plikten inntas i databehandleravtalen – se artikkel 30 om hva protokollen skal inneholde.

Databehandleravtalen skal være *skriftlig*, men den kan foreligge *elektronisk*, dvs. det er ikke noe krav at avtalen skal foreligge på papir.

Konsekvensene av at det ikke foreligger databehandleravtale, eller at avtalen ikke oppfyller lovens krav, er at databehandleren kan bli ansett å være behandlingsansvarlig og må ha grunnlag for behandling av personopplysninger. Foreligger det ikke databehandleravtale vil utlevering av personopplysninger fra den behandlingsansvarlige til databehandleren kunne være ulovlig. Dette er brudd på personopplysningsloven og GDPR, og i tillegg vil det faktum at det ikke foreligger databehandleravtale i seg selv være et brudd på loven. Ved brudd på loven kan Datatilsynet ilegge overtredelsesgebyr, og bøter og straff risikeres ved spesielt alvorlige forhold.