Den nye persondatabeskyttelsesforordning

Den 25. maj 2018 træder databeskyttelsesforordningen i kraft, og skal gælde for behandling af personoplysninger for alle borgerne i EU.

Personoplysninger defineres i forordningen som enhver information, der kan bruges til at identificere en bestemt fysisk person – såsom kunder, ansatte, mfl., f.eks. et navn eller et billede. Men også oplysninger, der indirekte, f.eks. ved sammenstilling af oplysninger med offentligt tilgængelig information eller med anden information hos den dataansvarlige virksomhed, kan identificere en fysisk person.

Alle virksomheder, myndigheder m.fl., der foretager en automatisk og/eller en manuel behandling af personoplysninger i et register (f.eks. en journal), skal overholde databeskyttelsesforordningen.

Kun registreringer til lovlige, rimelige og gennemsigtige formål

Enhver registrering og behandling af personoplysninger må kun finde sted, til

- udtrykkeligt angivne formål og legitime forhold

- må ikke viderebehandles på anden måde end formålet

- være tilstrækkelige og begrænset til, hvad der er nødvendigt i forhold til formålet

- være korrekte og ajourførte

- må ikke opbevares i længere tidsrum end det, der er nødvendigt til formålet

- skal opfylde kravene til sikkerhed og lovlig behandling.

Behandlingen af helbredsoplysninger

Hovedreglen er, at behandling af personoplysninger (følsomme oplysninger, herunder helbredsoplysninger) er forbudt.

Helbredsoplysninger defineres som personoplysninger, der vedrører en fysisk persons fysiske eller mentale helbred, herunder levering af sundhedsydelser, og som giver information om vedkommendes helbredstilstand.

Registrering og behandling af personoplysninger om jeres klienter skal derfor være lovlig, og kan derfor ske efter at I har modtaget et udtrykkeligt samtykke fra klienten.

Kravene til samtykke

Der skal være tale om en ”viljestilkendegivelse” fra jeres klient. Viljestilkendegivelsen skal være frivillig, specifik og informeret, og klienten skal give sit utvetydige ”ja”,

Som dataansvarlige skal du – som i dag – kunne påvise (bevise), at der foreligger et gyldigt samtykke. Der er ikke nødvendigvis et krav om skriftligt samtykke, men det er klogt at få et skriftligt samtykke, således at du til enhver tid kan påvise, at der foreligger et gyldigt samtykke.

Klienten har ret til at trække samtykket tilbage. Det er derfor en gyldighedsbetingelse for samtykket, at man har oplyst om tilbagetrækningsmuligheden.

Er et barn under aldersgrænsen (16 år er udgangspunktet i forordningen, men Datatilsynet kan fastsætte en lavere grænse) skal indehaveren af forældremyndigheden give samtykke på barnets vegne.

I forbindelse med indhentningen af samtykket skal I som minimum informere jeres klient om:

- Jeres identitet som dataansvarlige (dvs. virksomhedsnavn, adresse og CVR nr.)
- Formålet med den påtænkte behandling
- Hvilke oplysninger, der behandles
- Hvilken behandling, der finder sted (fysisk og digitalt)
- At samtykket til enhver tid kan trækkes tilbage.

Den registreredes rettigheder
Persondataforordningen giver den registrerede en række rettigheder, og de vigtigste rettigheder er

- Retten til at modtage oplysning om en behandling af sine personoplysninger (oplysningspligt)
- Retten til at få indsigt i sine personoplysninger (indsigtsret)
- Retten til at få urigtige personoplysninger berigtiget (retten til berigtigelse)
- Retten til at få sine personoplysninger slettet (retten til at blive glemt)
- Retten til at gøre indsigelse mod at personoplysninger anvendes til direkte markedsføring
- Retten til at gøre indsigelse (f.eks. klage til Datatilsynet)
- Retten til at flytte sine personoplysninger (dataportabilitet).

Behandlingssikkerhed

Forordningen stiller krav om en høj grad af sikkerhed ved behandlingen af personfølsomme oplysninger, både ved papirbaseret behandling (fx journalskrivning i hånden) og ved digital behandling (opdateret antivirus programmer, beskyttede passwords, rettighedsstyring (samt hvis større virksomhed en logning af alle brugernes handlinger/aktiviteter i programmet).

Følsomme personoplysninger, herunder helbredsoplysninger må kun transmitteres over internettet med sikker kryptering.

Dataansvarlig

Som dataansvarlig i din virksomhed, har du ansvaret for at etablere et sikkerhedsniveau, der kan beskytte imod risikoen for en overtrædelse af de registreredes rettigheder. I skal foretage en risikovurdering for at fastlægge det rette sikkerhedsniveau.

Hvis en behandling af personoplysninger er forbundet med en høj risiko for den registreredes rettigheder, skal I som dataansvarlig udarbejde en konsekvensanalyse, så I kan imødegå de pågældende ricisi.

I mindre virksomheder kan I dog nøjes med at udarbejde en analyse, der beskriver de konkrete og veldefinerede behandlinger, som er typiske for klinikken. Analysen skal indeholde retningslinjer rettet mod konkrete behandlingssituationer i det daglige arbejde, men skal også tage højde for evt. usædvanlige arbejdssituationer, som behandlingsaktiviteten måtte indgå i. Analysen skal fastsætte specifikke rammer for, hvordan man kan begrænse de ricisi, der er blevet identificeret i forhold til behandlingsaktiviteterne. Der skal også tages højde for, hvordan man kan følge op og foretage egenkontrol af virksomhedens aktiviteter over tid.

Hvad skal du gøre ved brud på sikkerheden

Hvis det går galt, og du som dataansvarlig i din klinik, bliver bekendt med et brud på persondatasikkerheden, skal du

- Påbegynde afhjælpning/standse sikkerhedsbruddet
- Uden unødig forsinkelse give besked til Datatilsynet inden 72 timer og
- Give besked til de personer, hvis oplysninger er berørt af sikkerhedsbruddet.

Som dataansvarlig kan du ifalde erstatningsansvar overfor de berørte fysiske personer samt modtage bøde fra Datatilsynet, hvis behandlingerne ikke opfylder kravene til sikkerhed og hvis der ikke er indgået en databehandleraftale med instruktioner til databehandler.

Datatilsynet barsler stadig med vejledning og standardbehandleraftaler på området, men forventes inden for de kommende måneder at have flere vejledninger på plads.

Hvis du vil vide mere

Vejledninger fra Datatilsynet

https://www.datatilsynet.dk/vejledninger/vejledninger-databeskyttelsesforordningen/

Privacy kompasset fra Erhvervsstyrelsen

https://erhvervsstyrelsen.dk/relancering-af-privacykompasset-hjaelp-til-de-nye-databeskyttelsesregler

Test om din virksomhed er klar til persondataforordningen via

https://startvaekst.virk.dk/privacykompasset/testen

Husk, at reglerne i forordningen er stadig genstand for præcisering, så følg løbende med i udviklingen.

Hvad kan ZCT gøre for at hjælpe

Foreningen kan hjælpe medlemmerne med at kunne påvise overensstemmelse med kravene i persondataforordningen, eksempelvis via følgende værktøjer:

- Udarbejde en adfærdskodeks til medlemmerne, som kan give fælles retningslinjer

    - Herunder klarhed over, hvilke typer registreringer kræves i forbindelse med journalføring
    - Hvilken information skal gives til klienterne, såvel før som ved indhentning af samtykke
    - Retningslinjer for ajourføring og sletning mm.

- Skabeloner til samtykkeerklæringer

- Afklare muligheden for supplerende forsikringer vedr. persondatabehandlingssikkerhed.

Alle medlemmerne opfordres dog hver især til at gennemgå egne persondatabehandlinger og foretage en risikoanalyse ifm. fysisk og digital behandlingssikkerhed. Det er vigtigt, at du giver gennemsigtig og tydelig information til klienterne om, hvad formålet med registreringen er, samt at du kan oparbejde processer for instruktioner og indgåelse af databehandleraftaler, sletning mm.