Regler for indhentning, behandling og opbevaring af personfølsomme data – GDPR

Den nye Persondataforordning (GDPR) har virkeligt sat mange på arbejde i forhold til at overholde de regler, der følger med. Og reglerne er skærpede i forhold til tidligere, selvom de fleste regler i virkeligheden har været der hele tiden. Men nu er tilsynet også skærpet og der udstedes nu bøder, såfremt vi ikke overholder reglerne. Bøderne er op til 4% af årlig omsætning.

Før har vi skullet tilmelde os Datatilsynet. Det skal vi ikke længere. I stedet skal du leve op til følgende krav:

Fortegnelse over behandleraktiviteter

Der skal for hver gruppe af ensartede persondata registreringer føres en fortegnelse over behandlingsaktiviteter. Denne fortegnelse skal du have liggende og kunne fremvise som dokumentation for, at du har taget stilling til datasikkerhed.

Der kan typisk være tale om følgende grupper:

- Medarbejderadministration
- Kundeadministration
- Leverandøradministration
- Overvågning

I praksis betyder det, at du skal lave oversigt over, hvordan du forholder dig til følgende:

Hvem og hvor?

- Hvilke kategorier af personer har du persondata om?
- Hvor i virksomheden registrerer du dem?

Lovlighed, rimelighed og gennemsigtighed

- Hvilke oplysninger har du registreret dette sted
- Er der tale om almindelige eller følsomme persondata?
- Hvilket grundlag har du for at registrere de pågældende persondata?
- Hvor kommer personoplysningerne fra?
- Hvem videregives persondata til?

- Hvem er ansvarlig for behandling af de registrerede persondata?
- Hvordan er den registrerede informeret om registreringen og den registreredes rettigheder?

Formålsbegrænsning

- Er der et legitimt formål med de registrerede persondata?
- Bruges de registrerede personoplysninger til andre formål?

Dataminimering

- Indsamles flere persondata end nødvendigt for formålet?

Rigtighed

- Hvorledes sikres, at de registrerede persondata er korrekte?

Opbevaringsbegrænsning

- Hvor/hvordan opbevares de anførte persondata?
- Hvornår slettes de anførte persondata?

Integritet og fortrolighed

- Hvordan sikres mod uautoriseret adgang til fysisk opbevaret persondata?
- Hvordan sikres mod uautoriseret adgang til elektronisk opbevaret persondata?

Ansvarlighed

- Hvorledes dokumenteres en overholdelse af persondatareglerne?

Risikovurdering

- Hvilke risici vurderes der at være vedrørende de registrerede persondata?

Se skema i bilag – "Behandleraktiviteter"

Samtykkekrav

Som behandler er du dataansvarlig. Som dataansvarlig skal du være klar og tydelig i din kommunikation, når du opbevarer eller på anden måde behandler dine klienters personoplysninger. Din klient skal altså have at vide, præcis hvad du opbevarer, hvorfor du opbevarer det og hvordan du har det opbevaret – og give sit udtrykkelige samtykke. Med udtrykkeligt menes, at der ikke kan sås tvivl om, hvorvidt samtykker reelt er afgivet.

Derfor er det vigtigt, at du informerer og får din klients udtrykkelige samtykke til følgende:

- Hvilke personoplysninger du registrerer
- Hvor du opbevarer dem
- Med hvilket formål personoplysningerne behandles
- Hvor lang tid personoplysningerne bliver opbevaret
- At din klient har ret til at få sine oplysninger berigtiget, slettet eller udleveret, samt få begrænset behandlingen heraf
- At din klient til enhver tid kan bede om at få oplysninger overført til anden databehandler
- At klienten til enhver tid kan trække sit samtykke tilbage, og hvordan dette kan ske
- Hvor din klient kan henvende sig for at gøre brug af sin ret til at få berigtiget, slettet eller udleveret – eller begrænset behandlingen af – sine oplysninger

Se eksempel på samtykkeerklæring under bilag – "Eksempel på Samtykkeerklæring"

Oplysningspligt

Du skal oplyse dine klienter (og andre), hvad du opbevarer, hvordan du behandler og hvordan du opbevarer oplysninger om dem i dit system. Dette kan du gøre i en såkaldt "Fortrolighedserklæring" – eller "Fortrolighedspolitik", som du har liggende på din hjemmeside eller udleverer til dine klienter og andre, der kommer i kontakt med dig.

Du skal desuden oplyse dem om, hvilke onlinetjenester, du benytter – og sikre dig, at disse lever op til kravene i GDPR.

Overførsel af data/journaler

Dine klienter skal have oplyst deres ret til at få overført alle data, journaler m.v. til andre systemer/tjenester.

Retten til at blive glemt

I din fortrolighedspolitik skal beskrives klientens ret til at blive glemt. Det betyder, at klienter til enhver tid kan bede dig om at slette alt, hvad du har liggende om dem. Dette gælder journaler, mails m.v.

Du har dog pligt til at gemme oplysninger, der er gemt i dit regnskabssystem i 5 år, ifølge loven.

Retten til at sikre korrekte oplysninger, få indsigt eller begrænse oplysninger

Din klient har ret til at få verificeret, at det er de rigtige oplysninger, du har liggende om dem – og få dem ændret, hvis de er forkerte. Desuden har de ret til at kræve, at du begrænser informationerne, hvis de ønsker det. Dette skal du også oplyse dem om.

Hvor længe gemmes oplysninger

Du skal informere dine klienter om, hvor længe du opbevarer oplysningerne, du har om dem. Det gæler både journaler og de oplysninger, der skal gemmes i dit regnskabsprogram.

Klagemuligheder

Din klient skal gøres opmærksom på, at de kan klage til Datatilsynet, hvis de oplever, at du ikke lever op til kravene.

Du kan se eksempel i bilag – "Eksempel på Fortrolighedspolitik"

Kommunikation med dine klienter

Du skal oplyse dine klienter om (og efterleve naturligvis), at al kommunikation fra dig foregår sikkert. Det betyder, at du bør kryptere dine mails, når der er personfølsomme oplysninger involveret. Og det ER der, så snart det er klart, at vedkommende du kommunikerer med, går i terapi hos dig. Det alene er personfølsomt.

I forhold til at kommunikere på facebook/messenger, så foreligger der ikke noget klart i forordningen/lovgivningen. Men da det d.d. ikke er en sikker måde at kommunikere på, og efter en snak med Datatilsynet, vurderer vi, at Tobias-Skolen ikke vil anbefale, at kommunikation med klienter foregår via messenger. Og selvom du kan få din klients samtykke til, at kommunikation foregår derigennem, vil det **ALTID være dit ansvar at dokumentere sikkerheden**, og det vil **altid være dig, der bliver stillet til ansvar** i tilfælde af "besøg fra Datatilsynet".

Derfor anbefaler vi at bruge e-mail og få installeret en krypteringsmulighed.

Og hvad med telefon?

Hvis du bruger en smartphone, og du har diverse sociale App's liggende på den (facebook, snapchat, Instagram og lign.), så må du faktisk ikke bruge din telefon til kommunikation med klienter. Disse App's har adgang til dine kontakter, og klienter må ikke blive identificeret via dig. Faktisk må ingen få mistanke eller informationer om, at klienter går i terapi hos dig.

Så ud fra dette, kan vi kun anbefale, at du får en arbejdstelefon og holder den fri for alle former for App's, der ikke er relevante i dit arbejde.

Opbevaring af data/journaler

Du skal opbevare dine data/journaler forsvarligt.
Hvis du har fysiske journaler, skal disse låses inde og de må ikke efterlades i rum, hvor der kommer andre end dig. Når du forlader rummet, skal de låses inde. Hvis der kommer andre i rummet, skal du have alle dokumenter liggende med bagsiden opad.

Har du oplysninger liggende på computeren, skal der være kode på, og din computer skal låses med kode, hver gang du forlader den.

Benytter du online-backup eller opbevarer du oplysninger online, skal du sikre dig, at de tjenester, du benytter, lever op til kravene.

Som eksempel på et system med helt styr på sikkerheden og GDPR kan nævnes "Terapeutbooking.dk".

Hvis du gemmer "i skyen", skal det som sagt være GDPR-sikrede systemer. Google-drev er f.eks. ikke GDPR-sikkert, som det ser ud lige p.t. Og det samme gælder Dropbox. Derimod er Office365 (OneDrive) sikkert.

Du skal have en databehandleraftale liggende på de tjenester, du benytter.

Nyttige links

www.datatilsynet.dk

https://www.datatilsynet.dk/media/6559/generel-informationspjece-om-databeskyttelsesforordningen.pdf
Datatilsynets side om Persondataforordningen

https://www.datatilsynet.dk/media/6562/samtykke.pdf
Datatilsynets beskrivelse af Samtykke

https://www.dp.dk/wp-content/uploads/spoergsmaal-om-datasikkerhed.pdf
Dansk Psykologforenings beskrivelse af GDPR/Persondataforordningen

http://www.dp.dk/radgivning/selvstaendige-psykologer/datasikkerhed/
Dansk Psykologforenings FAQ om GDPR