Den nye persondataforordning

Den nye persondataforordning træder i kraft den 25. maj 2018, og er en forordning som skal ensarte reglerne om databeskyttelse på det europæiske marked. Danmark har allerede en relativt høj beskyttelse som følge af den gældende Persondatalov, men forordningen vil medføre yderligere stramninger.

Persondataforordningen gælder alle, som håndterer persondata og medfører, at der vil komme større fokus på, hvordan virksomheder håndterer data, både hvad gælder medarbejderdata og f.eks. klientdata. Den medfører skærpede krav omkring samtykke og indeholder også en regel om, at man har ret til at blive glemt, dvs. at såfremt man kræver det, skal data i nogle tilfælde kunne slettes.

Den nye forordning bliver direkte gældende i dansk lovgivning, men indeholder også muligheder for nationale fortolkninger, hvilket vil medføre, at der i praksis vil være tale om en blanding af forordning, dansk lovgivning og praksis. Vi kan endnu ikke se det endelige resultat, idet det kræver, at Danmark først har implementeret de dele af forordningen, som medfører pligt eller mulighed for supplerende national lovgivning.

Nogle af de større ændringer, som persondataforordningen medfører, er de skærpede samtykkeregler, at offentlige myndigheder og visse private virksomheder skal udpege en databeskyttelsesansvarlig, at bødeniveauet for brud mod databeskyttelsesregler er meget højere end tidligere, og at der foreligger højere dokumentationskrav for dataflow, herunder også at man skal informere relevante myndigheder om eventuelle brud på datasikkerheden.

Hvad er en personoplysning?

En personoplysning er et overordnet begreb, der omfatter alle oplysninger, som kan henføres til en bestemt fysisk person, såsom navn og alder, men også personfølsomme oplysninger såsom helbredsoplysninger. Det gælder også oplysninger, som først i kombination med andre oplysninger kan henføres til en bestemt fysisk person. Enkeltmandsvirksomheder omfattes også af begrebet, idet de oplysninger kan henføres til en ejer.

Hvad er en personfølsom oplysning?

En personfølsom oplysning er en oplysning om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold. Med den nye forordning omfattes også genetiske og biometriske* data.

*biometriske data: personoplysninger om fysiske karakteristika, såsom ansigtsbillede eller fingeraftryksoplysninger.

Er et navn en personfølsom oplysning?

Nej, et navn er ikke i sig selv en personfølsom oplysning, men en personoplysning. Dog – såfremt navnet medfører en identificering af en person i en personfølsom sammenhæng (i kombination med andre oplysninger), f.eks. at man kan se, at en navngiven person skal deltage i en psykologisk undersøgelse - så skal det behandles med tilstrækkelige sikkerhedsforanstaltninger.

Kan man indhente samtykke fra en klient/person som skal deltage i en psykologisk undersøgelse vedrørende at man kommunikerer via mail som ikke er krypteret?

Nej, ansvaret for at personfølsomme data ikke kommer i uvedkommendes kendskab ligger hos den dataansvarlige, dvs. i dette tilfælde psykologen, og kan ikke samtykkes væk af den, der er i behandling.

Hvad er en dataansvarlig?

En dataansvarlig er en fysisk eller juridisk person*, offentlig myndighed, institution eller andet organ, som alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af oplysninger. Den dataansvarlige er lovens primære pligtsubjekt, hvilket også medfører, at det er den dataansvarlige, som har det overordnede ansvar, også for behandling af data, som foretages af tredjemand på vegne af den dataansvarlige.

*Juridisk person: en virksomhed

Hvad er en databehandler?

En databehandler er enhver, som behandler oplysninger på vegne af en dataansvarlig. Som eksempler kan nævnes virksomheder, som varetager drift af kunders it-systemer, eller hostingvirksomheder som f.eks. tilbyder serverkapacitet til indehavere af hjemmesider.

Skal en privatpraktiserende psykolog tilmelde sig Datatilsynet i forbindelse med behandling af personfølsomme oplysninger?

Nej, en privatpraktiserende psykolog er ikke forpligtet til at tilmelde sig Datatilsynet i forbindelse med behandling af personfølsomme oplysninger. Dette følger af en undtagelsesbestemmelse i persondataloven, som medfører, at autoriserede psykologer, som arbejder indenfor sundhedsområdet, ikke omfattes af kravet om tilmelding, ligesom f.eks. læger heller ikke omfattes.

Er det sikkert at udføre internetbaseret terapi via Skype eller FaceTime?

Nej, det er vores opfattelse, at Skype og FaceTime, eller lignende internetbaserede telefonkonferenceprogrammer, ikke er sikre nok. Dette skyldes, at data ikke er tilstrækkeligt beskyttet, herunder er serverne placeret udenfor EU, hvorfor der ikke gælder samme lovgivning omkring datasikkerhed.

Der findes nogle internetbaserede løsninger, der garanterer sikre forbindelser, men hvis man benytter sig at disse, skal man selv sikre sig, at sikkerheden lever op til lovgivningen.

Ansvaret for at personfølsomme data ikke kommer i uvedkommendes kendskab ligger hos den dataansvarlige, dvs. i dette tilfælde psykologen. Ansvaret kan – ligesom i forbindelse med at man som psykolog mailer med en klient – ikke samtykkes væk af den, der er i behandling.

Er internetservere sikre?

Du kan have en egen server, som er sikret, ellers skal du have databehandleraftaler hele vejen ned til den sidste i databehandlerkæden, som kan dokumentere sikkerheden.

Hvilke krypteringskrav gælder for mail?

Ligesom ved internetbaseret terapi ligger ansvaret for at personfølsomme data ikke kommer i uvedkommendes kendskab hos den dataansvarlige, dvs. i dette tilfælde psykologen. Ansvaret kan ikke samtykkes væk af den, der er i behandling. Det er dig som psykolog, som har ansvaret for, at mail og indholdet er tilstrækkeligt sikret.

Hvordan kan man udføre sikker kommunikation med klienter og andre interessenter? Må man indkalde til psykologisk undersøgelse via mail?

Indholdet i korrespondance med klienter vil oftest være at betegne som personfølsomme oplysninger og skal derfor sikres. Dette gælder både oplysninger omkring klienter samt indholdet fra behandling.

Såfremt opgaven udføres på vegne af en kommune (en offentlig myndighed), er du som psykolog omfattet af sikkerhedsbekendtgørelsen, idet du i det tilfælde agerer som databehandler for kommunen. Dette medfører, at du skal sikre informationen med kryptering.

Såfremt du udfører opgaven privat, dvs. ikke på vegne af en offentlig myndighed, skal du stadig følge vilkårene i persondatalovens § 41. Der foreligger i den forbindelse ikke et udtalt krav, men en klar anbefaling fra Datatilsynet om, at personfølsomme oplysninger bør krypteres.

Hvornår skal jeg så som psykolog sende krypterede mails?

Når en klient kontakter dig via mail, kan du ikke være sikker på, om forbindelsen er krypteret. Ved besvarelse skal du derfor skrive en ny krypteret mail fra din egen sikre e-mailadresse som svar. Derfor skal du altså ikke svare direkte på den oprindelige mail.

Det anbefales desuden, at du minder klienten om ikke at sende personfølsomme oplysninger til dig via en ikke-krypteret e-mail.

Må man modtage betaling via bankoverførsler eller MobilePay?

Ja, det er bankens ansvar at sikre, at bankoplysninger behandles fortroligt, og det er derfor ikke noget problem, at klienter betaler via bankoverførsel eller MobilePay.

Må man som psykolog opbevare data på DropBox?

Nej. Ved at opbevare data på en internetserver gives der adgang til data for tredjeparter. Hvis data ikke opbevares i et europæisk land, er virksomheden ikke omfattet af den europæiske lovgivning for datasikkerhed (se også Datatilsynets hjemmeside: https://www.datatilsynet.dk/erhverv/tredjelande/oeverfoersel-til-tredjelande/). Dette betyder, at gratistjenester som DropBox ikke kan benyttes.

Er oplysninger i min klientkalender personfølsomme oplysninger?

Ja, det er en personfølsom oplysning, at en klient går til en psykolog. Det skal derfor sikres, at dette ikke kan læses ud af din kalender. Har du en elektronisk kalender på din smartphone, iPad eller lignende, skal du derfor sikre dig, at f.eks. synkronisering ikke sker til en usikret internetserver, men kun til en sikret internetserver eller sikret computer.

Hvordan sikrer jeg, at indholdet i min kalender overholder regler om beskyttelse af persondata?

En måde at holde kalender på er ved at skrive initialer, listenummer eller lignende i din kalender, og så have en liste med faktiske navne liggende et sikkert sted, eksempelvis lokalt på en computer, som kun du har adgang til.

Må jeg bruge min smartphone/iPad/tablet til både arbejde og privat?

Nej. Problemet med smartphones er, at mange apps beder om at få adgang til data på telefonen, hvilket gør, at eksterne aktører kan få fat i det data, der måtte være på telefonen. Til privat brug vil du derfor typisk have flere apps, der kan få adgang til de følsomme oplysninger, som ligger fra dit arbejde.

Må jeg sikkerhedskopiere min smartphone/iPad/tablet?

Kun hvis du sikkerhedskopierer til en sikret computer eller server. Du må f.eks. altså ikke gemme på en ”cloud”.

Må jeg kommunikere med klienter via sociale medier, f.eks. Facebook?

Nej. Du må ikke kommunikere med dine klienter over sociale medier som Facebook, da al data, som går igennem sådanne sider, tilhører ejerne af siderne. Dette betyder, at alt det, du skriver på Facebook, bliver gemt hos en tredjepart, der kan bruge det, som de har lyst. Dette gælder både private beskeder via sociale medier, samt kommentarer til andres opslag på sociale medier.