Procedure for håndtering af personoplysninger - GDPR

Denne udgave: 23.08.2018/TW

DolphinEyes® ApS (i det følgende virksomheden) beskriver med denne procedure, hvordan vi opfylder persondataloven.

Proceduren er udfærdiget baseret på vejledningen: "Databeskyttelsesforordningen. En introduktion til de kommende, nye regler om beskyttelse af personoplysninger" (Erhvervsstyrelsen, Digitaliseringsstyrelsen, Justitsministeriet og Datatilsynet, 2017).

Definitioner

Dataansvarlig

I denne procedure er beskrevet retningslinjer, der gælder for DolphinEyes

Databehandlere

Konsulenter, underleverandører og andre organer, der behandler personoplysninger på virksomhedens vegne og efter instruks fra virksomheden.

Formålsbegrænsning

Når der indsamles oplysninger i virksomheden, skal den dataansvarlige gøre sig klart, hvilke formål oplysningerne indsamles til, og det skal være saglige formål. Om formålene er saglige bedømmes ud fra, om indsamlingen sker i forbindelse med løsningen af en opgave, som det er naturligt for virksomheden at løse.

Virksomheden må ikke indsamle oplysninger med den begrundelse, at det måske senere kan vise sig nyttigt at være i besiddelse af oplysningerne. Det er i første omgang den virksomhed eller myndighed mv., der indsamler oplysninger, som skal vurdere, om en bestemt indsamling af oplysninger er saglig.

Rigtighed

Den dataansvarlige skal sikre sig, at oplysningerne er rigtige og ajourførte. Hvis oplysningerne viser sig at være urigtige, skal de som udgangspunkt slettes eller berigtiges.

Opbevaringsbegrænsning

Personoplysninger slettes eller gøres anonyme, når det ikke længere er nødvendigt for den dataansvarlige at have oplysningerne. Det er op til virksomheden at vurdere, hvor længe det er nødvendigt at opbevare oplysningerne ud fra det formål, som oplysningerne oprindelig blev indsamlet til.

Integritet og fortrolighed

Personoplysninger der registreres skal beskyttes mod uautoriseret eller ulovlig behandling, ligesom det skal sikres, at oplysninger ikke går tabt eller bliver beskadiget.

Computere og databaser der anvendes af virksomheden og de tilknyttede databehandlere skal være beskyttet med robuste passwords. De skal desuden sikkerhedsopdateres jævnligt.

Følsomme personoplysninger

Virksomheden registrerer IKKE følsomme oplysninger om fysiske personer eller enkeltmandsvirksomheder, med mindre det foregår efter en klinisk protokol godkendt af Datatilsynet i det pågældende land.

Følsomme oplysninger hidrører race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Oplysninger om strafbare forhold

Virksomheden registrerer IKKE strafbare oplysninger om fysiske personer eller enkeltmandsvirksomheder.

Oplysninger om strafbare forhold kan være en oplysning om, at en person har begået en bestemt lovovertrædelse, men det kan også f.eks. være en oplysning om, at en person har adresse i et fængsel.

Oplysninger om CPR-nummer

Virksomheden registrerer udelukkende CPR numre på fysiske personer, der er ansat i virksomheden, i de tilfælde hvor der er en arbejdsgiverpligt til at gøre dette (lønsystemer eller lignende). Personfølsomme oplysninger registreret i lønsystemer indhentes fra personerne selv direkte, og det vil fremgå af dialogen hvad formålet med oplysningerne skal bruges til.

Almindelige personoplysninger

Virksomheden vil i visse tilfælde registrere almindelige personoplysninger, f.eks. identifikationsoplysninger som navn og adresse, oplysninger om økonomiske forhold, kundeforhold eller andre lignende ikke-følsomme oplysninger. Registreringerne foregår efter vejledningerne beskrevet i denne procedure:

- Den person, der behandles oplysninger om, skal som udgangspunkt have oplyst, hvem der er ansvarlig for behandlingen af oplysninger, og hvad der er formålet med behandlingen, om eventuelle modtagere af oplysningerne, mv.
- Det vil være forskelligt hvordan information om databehandling oplyses til personer, der behandles oplysninger om.
    - Almindelige personoplysninger, der registreres i et CRM arkiv med henblik på mødeplanlægning, interessetilkendegivelser og lignende (professionelle

kontaktoplysninger, datoer for kontakter mv): Ved korrespondance med personer, der registreres i CRM arkiv gøres opmærksom på hvilke forhold vi noterer, og hvorfor vi gør det. Eksempel: En kundesupportmedarbejder på en øjenklinik spørges om standard forsigtighedsregler efter operation for grå stær. Hun bliver spurgt om det er i orden at hendes navn nævnes i en ansøgning om fondsmidler, da vi er afhængige af at eksperter fra feltet giver deres mening til kende. Dette siger hun ja til, hvorefter det skrives ind i ansøgningen. Medarbejderens fornavn, kundesupports telefonnummer og en kort note om samtalen nedskrives efterfølgende i CRM arkivet.

- Almindelige personoplysninger, der fremgår af mødereferater og lignende: Som ovenfor gøres personer opmærksomme på at der skrives referat, og til hvilket formål. Almindelige personoplysninger, der fremgår af ansættelseskontrakter, samarbejdsaftaler og lignende: Her vil personerne oftest være medunderskrivere af dokumenterne, hvorfor det giver sig selv hvad formålet er med informationerne. Informationerne må ikke bruges til andre formål end de aftalte uden at personerne orienteres om det.
- Almindelige personoplysninger, der fremkommer ved at aflæse cookies på virksomhedens kommende hjemmeside: På virksomhedens hjemmeside vil der, når den tilgås, dukke en enkel og forståelig besked op. I beskeden orienteres læseren om at der skal give sit samtykke til at oplysningerne benyttes på den måde, der fremgår af virksomhedens oplysninger om privatlivspolitik. Læseren skal have oplysning om, at samtykket kan trækkes tilbage, og det skal være lige så let at trække samtykket tilbage som at give det. Oplysningerne om privatlivspolitik er tilgængelige på hjemmesiden. Hvis brugeren af hjemmesiden IKKE giver sit samtykke, vil persongenkendende cookies ikke blive registreret. Hvis brugeren trækker sit samtykke tilbage, skal virksomheden oplysninger på grundlag af samtykket slettes.

De registreredes rettigheder

På virksomhedens hjemmeside er et afsnit tilgængeligt for brugerne om privatlivspolitik. I afsnittet anføres de vigtigste rettigheder:

- 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 mod automatiske individuelle afgørelser, herunder profilering
- Retten til at flytte sine personoplysninger (dataportabilitet)

Hvis en person henvender sig til den virksomheden og f.eks. beder om indsigt, berigtigelse, sletning, mv. af oplysninger, skal den pågældende hurtigst muligt – og normalt senest efter en måned – have besked om, hvad der vil blive gjort som følge af henvendelsen.

Om nogle af rettighederne kan særligt fremhæves følgende:

Ret til at få besked om, at der behandles personoplysninger (oplysningspligt)

Den enkelte registrerede skal som udgangspunkt have besked om, at der behandles oplysninger om den pågældende. Man skal bl.a. have besked om, hvem der er dataansvarlig, om formålet med behandlingen, om eventuelle modtagere af oplysningerne, mv.

Ret til at se oplysninger (indsigtsret)

Den registrerede kan bede om at få at vide, hvilke oplysninger om den pågældende selv, som en myndighed eller virksomhed mv. behandler. Hvis den registrerede beder om det, skal der også gives en udskrift eller kopi af oplysningerne.

Ret til at få oplysninger rettet eller slettet (retten til at blive glemt)

Hvis der behandles forkerte oplysninger om en person, kan den pågældende bede om at få oplysningerne rettet. Desuden har man i visse tilfælde ret til at få personoplysninger slettet. Det kan f.eks. være, hvis oplysningerne ikke længere er nødvendige til at opfylde de formål, hvortil de blev indsamlet, hvis et samtykke, som er nødvendigt for behandlingen, trækkes tilbage eller hvis behandlingen er ulovlig.

Ret til at transmittere oplysninger (dataportabilitet)

Den registrerede har ret til at modtage personoplysninger om sig selv i et struktureret, almindeligt anvendt og maskinlæsbart format og har ret til at transmittere oplysningerne til en anden myndighed eller virksomhed. Den registrerede kan også bede om at få oplysningerne sendt direkte fra den dataansvarlige til en anden myndighed eller virksomhed.

Behandlingssikkerhed

Brug og håndtering af personoplysninger skal foregå betryggende og med et passende niveau af sikkerhed og privatlivsbeskyttelse. Sikkerhedsniveauet skal afspejle den konkrete risiko for, at oplysningerne stjæles, mistes, skades, eller behandles ulovligt.

Hvis risikoen må antages at være stor, må behandlingen af personoplysninger ikke påbegyndes, før der er gennemført en konsekvensanalyse vedrørende databeskyttelse og eventuelt en høring af Datatilsynet.

Hvis der eksempelvis skal foretages en brugertest, hvor der forventes at inkluderes følsomme oplysninger, skal protokollen forhåndsgodkendes af Datatilsynet. Se i øvrigt næste afsnit om Konsekvensanalyser.

Når it-løsninger designes og udvikles, skal databeskyttelse tænkes ind fra starten, og standardindstillinger skal sikre, at der kun behandles de personoplysninger, som er nødvendige i forhold til formålet med behandlingen.

Hvis det går galt, og man som dataansvarlig bliver bekendt med et brud på person-datasikkerheden, skal man uden unødig forsinkelse give besked til Datatilsynet og i visse tilfælde også til de personer, hvis oplysninger er berørt af sikkerhedsbruddet. Databehandlere, som bliver

bekendt med et brud på persondatasikkerheden, skal uden unødig forsinkelse underrette den dataansvarlige.

Konsekvensanalyser

Virksomheden skal foretage en konsekvensanalyse forud for databehandlinger, som sandsynligvis vil indebære en høj risiko.

Formålet med konsekvensanalysen er navnlig at vurdere risikoens oprindelse, karakter, særegenhed og alvor.

Det vil bl.a. være relevant at foretage en konsekvensanalyse i tilfælde, hvor nye teknologier anvendes, eller hvor der behandles meget store mængder følsomme personoplysninger.

Analysen skal mindst omfatte:

Systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen,
En vurdering af, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene,
En vurdering af de risici behandlingen indebærer for de personer, der behandles oplysninger om, garantier, sikkerhedsforanstaltninger og mekanismer, der skal sikre beskyttelse af personoplysninger og påvise overholdelse af databeskyttelsesforordningen.

Datatilsynets vejledning kan benyttes til at strukturere og gennemføre analysen.

Denne procedure er oprettet den 23. august 2018 af Trine Wulff

Godkendelse:

Helle Kayerød, CEO, DolphinEyes® ApS

Dato