Definitioner og begreber

I dette afsnit kan du finde definitioner på en række centrale begreber i persondataforordningen.

Den registrerede

Den registrerede er den person, som personoplysningerne er knyttet til. På en institution vil det fx være børn, medarbejdere, forældre, samarbejdspartnere, mv. Hvis en person er under 18 år, er det forældremyndighedsindehaveren/-haverne, der skal give samtykke til behandling af oplysninger på den registreredes vegne. Dog bør og kan børn og unge i nogle tilfælde selv give samtykke til behandling af deres personoplysninger, se nærmere herom under Forældreansvarsloven og persondata.

Dataansvarlig

Den dataansvarlige er en arbejdsgiver, som fx en institution, der behandler personoplysninger (f.eks. indsamling, registrering og videregivelse) om sine ansatte og børn, mfl. Det er den dataansvarlige, der har ansvaret for, at personoplysningerne behandles i overensstemmelse med Persondataforordningens krav og at eventuelle databehandlere, som behandler oplysninger på den dataansvarliges vegne, overholder relevante krav til sikkerhed, mv.

Databehandler

En dataansvarlig kan vælge at overlade det til en anden at udføre den praktiske behandling af personoplysninger på sine vegne. En databehandler kendetegnes ved kun at behandle personoplysninger på vegne af (efter instruks fra) en dataansvarlig. Databehandleren behandler aldrig personoplysninger til egne formål og må derfor ikke bruge de tilgængelige oplysninger til andet end udførelsen af opgaven for den dataansvarlige. I praksis kan en databehandler f.eks. være en virksomhed, som varetager en institutionens it-systemer. En databehandler kan også være en udbyder af et webhotel, der hoster hjemmesider for andre, eller et inkassobureau, som overlades oplysninger fra en dataansvarlig med henblik på inddrivelse af gæld. Det er ikke afgjort i Persondataforordningen om rådgivning fra fx advokater, revisorer, fobu og kommuner skal omfattes af databehandleraftaler. Vi håber, at der vil komme afklaring på dette spørgsmål i en af de yderligere vejledninger, som ventes fra Justitsministeriet om fortolkning af forordningen.

Personoplysninger

En personoplysning er enhver form for information om en identificeret eller identificerbar fysisk person (barn, forældre, ansat, samarbejdspartner mv.).

Personen skal direkte eller indirekte kunne identificeres gennem oplysninger, som er særlige for personens identitet, som fx navn, cpr.nummer, adresse eller online-identifikatorer som fx ip-adresser. Billeder fra fx tv-overvågningsudstyr er også persondata, som derfor er reguleret ved persondataforordningen.

Forordningen skelner mellem to kategorier af personoplysninger:

• **Almindelige oplysninger** er fx navn, adresse, stilling, indkomst og formueforhold, civil stand, sygedage, tjenstlige forhold, eksamen, ansøgning, CV, strafbare forhold, væsentlige sociale problemer, andre rent private forhold, som fx bortvisning fra jobbet. Disse er oplysninger, som man gerne må

behandle, hvis man har fået personens samtykke hertil eller institutionen ved lov er forpligtet til at behandle oplysningerne.

• **Følsomme oplysninger**, er information om personen, som det iflg. forordningen er forbudt at registrere. Det gælder racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, samt medlemskab af fagforening og helbredsmæssige eller seksuelle forhold.

• Det er kun muligt at få dispensation fra forbuddet mod registrering af følsomme oplysninger, hvis der er tale om et helt specifikt formål og personen har givet **udtrykkeligt samtykke** til behandlingen.

Behandling

Behandling er enhver håndtering af oplysninger, dvs. alle de måder, institutionen behandler oplysninger på. Behandling er altså enhver indsamling, registrering, systematisering, opbevaring, ændring, søgning, transmission, videregivelse, sammenstilling, samkøring, blokering, sletning eller tilintetgørelse af oplysninger. Det er fx registrering af ansøgere til ventelister, overførsel af oplysninger til andre aktører, udbetaling af løn, registrering af sygefravær og oplysninger, som indtastes i fobus lønprogrammer. Persondataforordningen gælder for alle typer af databehandling, dvs. både elektronisk og manuel behandling, dvs. emails, indtastning i registre og økonomisystem, systemoverførsler til fx optagelse.dk eller andre databaser, fysiske breve, notater fra telefonsamtaler, mv.

Samtykke

Personen, hvis oplysninger bliver behandlet og opbevaret, skal give samtykke hertil. Samtykket kan når som helst trækkes tilbage. Samtykket er ikke længere gyldigt, hvis formålet med behandlingen af oplysninger ændrer sig, eller der slet ikke er et formål længere.

Samtykket skal være en tydelig tilkendegivelse af, at vedkommende er indforstået med behandlingen og opbevaringen. Samtykket skal være **skriftligt** og skal desuden være:

• **Tydeligt adskilt fra den øvrige tekst** – Må eksempelvis ikke være skjult som en del af teksten, skrives med småt eller lignende.

• **Være frivilligt** – Der skal være et reelt frit valg til afgivelse af samtykke. En aftale/kontrakt må ikke være betinget af afgivelse af samtykke til behandling af oplysninger, som ikke er nødvendige.

• **Specifikt** – Det skal specificeres hvilke oplysninger, der gives samtykke til behandling af.

• **Informeret** – Der skal gives oplysninger om, hvad samtykket indebærer, og om retten til at **tilbagekalde** sit samtykke.

• **Utvetydigt/udtrykkeligt** – Der må ikke kunne være tvivl om, hvorvidt der er afgivet samtykke til behandling af de specifikke oplysninger. Hvis man anmoder om samtykke til behandling af følsomme, skal de specifikke formål med indsamlingen til hver enkelt oplysning fremgå af samtykket.

Den registreredes rettigheder

Den registrerede har en række rettigheder, som udmønter sig i forpligtelser for den dataansvarlige. Det vil sige, at institutionen aktivt skal foretage en række handlinger for, at disse rettigheder kan siges at være opfyldt. **Oplysningspligten**, dvs. pligten til at oplyse personen om behandlingen af personoplysninger, er forskellig afhængigt af, om oplysningerne kommer fra personen selv eller en tredjepart.

Databehandleraftale

Når man lægger behandlingen af data ud til en databehandler kræver det, at der indgås en skriftlig aftale mellem den dataansvarlige og databehandleren. Det kaldes en databehandleraftale. Det er institutionens, dvs. dataansvarliges ansvar, at aftalen er indgået. Det skal fremgå af aftalen, at databehandleren alene handler efter instruks fra den dataansvarlige, og at databehandleren skal opfylde en række tekniske og organisatoriske sikkerhedskrav. Disse sikkerhedsforanstaltninger skal sikre mod, at oplysningerne forsvinder, misbruges eller på anden måde behandles i strid med lovgivningen. Det er et område med stor vægt i Persondataforordningen og derfor noget, databehandlerne selv bør bidrage aktivt til at opfylde.

Data Protection Officer(DPO) eller Databeskyttelsesrådgiver

En Data protection officer (DPO) er en medarbejder i den dataansvarlige organisation, som udnævnes til at varetage opgaven med at sikre, at man lever op til Persondataforordningens krav. Iflg. Justitsministeriets udmeldinger gælder kravet om at udnævne en person for offentlige myndigheder, som er omfattet af forvaltningslovens § 1. Selvejende institutioner vil som følge af deres driftaftale/driftsoverenskomst være underlagt forvaltningsloven, og skal derfor udpege en databeskyttelsesrådgiver.

Konsekvensanalyse – Data Protection Impact Assessment (DPIA)

Persondataforordningen stiller krav om, at dataansvarlige organisationer i visse tilfælde udarbejder en konsekvensanalyse af brud på datasikkerheden. Det gælder primært myndigheder, som træffer afgørelser på baggrund af elektronisk registrering eller hvis der behandles følsomme oplysninger i stort omfang (fx et hospital) eller data kommer fra overvågning af offentlige områder.

Selvom det pt. vurderes at institutioner vil blive udsat for krav om udformning af konsekvensanalyser, kan det alligevel være en god idé at forholde sig til, om de data, institutionen behandler om barnet er af særlig privat karakter således, at det vil være forbundet med væsentlige omkostninger for barnet, hvis data kommer til uvedkommendes kendskab. I de tilfælde, hvor sådanne data behandles, er det særlig relevant at overveje sikkerheden ved opbevaring af data og ved overførsel af data til tredjepart. Det kan fx dreje sig om PPR-vurderinger, oplysninger fra sundhedsplejerske eller læge, notater til brug for underretninger til kommunen, notater om konflikter i familien, mv.