20-04-2020

Bilag 2 - GDPR-ordbog (i alfabetisk rækkefølge)

Anonymisering: En handling, som gør, at oplysninger ikke længere kan føres tilbage til en identificerbar eller identificeret fysisk person. Oplysninger, der er gjort anonyme, sådan at ingen fysiske personer kan identificeres ud fra oplysningerne, ej heller hvor disse kombineres med andre oplysninger, er ikke længere beskyttet af databeskyttelsesreglerne. Det skyldes, at databeskyttelsesreglerne kun finder anvendelse, så længe oplysningerne kan føres tilbage til en identificerbar eller identificeret fysisk person.

Awareness: Handler om at skabe opmærksomhed blandt medarbejderne omkring behandling og beskyttelse af personoplysninger.

Behandling (databeskyttelsesretlig sammenhæng): Begrebet behandling skal i databeskyttelsesretlig sammenhæng forstås meget bredt og omfatter enhver aktivitet eller række af aktiviteter, som personoplysninger gøres til genstand for fra det tidspunkt, hvor oplysningerne opstår eller indsamles til det tidspunkt, hvor de ophører med at være personoplysninger gennem sletning eller anonymisering.
Eksempler på (data)-behandling er:
- Indsamling
- Registrering
- Organisering
- Systematisering
- Opbevaring
- Tilpasning eller ændring
- Genfinding
- Søgning
- Brug
- Videregivelse
- Overladelse
- Sammenstilling eller samkøring
- Begrænsning
- Sletning eller tilintetgørelse

Compliance: Efterlevelse/overholdelse af regler f.eks. i GDPR.

Dataansvarlig: Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ der afgør til hvilket formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger.

Databehandler: Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ der behandler oplysninger på den dataansvarliges vegne. Databehandleren handler udelukkende på baggrund af en instruks fra den dataansvarlige, og databehandleren må ikke selv disponere over personoplysningerne eller benytte disse til egne formål. Det kan f.eks. være en leverandør af et it-system, hvori der behandles personoplysninger.

Databehandleraftale: En skriftlig aftale, der indgås mellem den dataansvarlige og en databehandler for at sikre at persondata beskyttes og behandles korrekt.

Dataminimering: Man må kun indsamle tilstrækkelige, relevante og nødvendige data om personer. Der må således ikke indsamles data, der er unødvendige i forhold til formålet, samtidigt med at behandlingen af data skal ske på et egnet grundlag. Der skal derfor, når der indsamles oplysninger, ske en konkret vurdering af hvilke data, der er relevante for at opfylde formålet med indsamlingen.

Fortegnelse (oversigt over behandling af personoplysninger): Vi har pligt til at udarbejde en fortegnelse over alle de aktiviteter i kommunen, som indebærer behandling af persondata. En sådan fortegnelse giver overblikket over kommunens behandlingsaktiviteter, hvori det bl.a. er beskrevet hvilke oplysninger, der behandles, hvad formålet med behandlingen er og hvilket retsgrundlag (hjemmel) de behandles på.

Konsekvensanalyse (DPIA): En konsekvensanalyse vedrørende databeskyttelse er en proces, der har til formål at beskrive behandlingen, vurdere dens nødvendighed og proportionalitet og bidrage til at håndtere de risici for fysiske personers rettigheder og frihedsrettigheder, som behandlingen af personoplysninger medfører ved at vurdere dem og fastlægge foranstaltninger til at afhjælpe dem.

En konsekvensanalyse skal således ses i sammenhæng med risikovurderingerne (se nedenfor), da man som dataansvarlig alene har pligt til at foretage en konsekvensanalyse i de tilfælde, hvor der sandsynligvis er høj risiko for fysiske personers rettigheder og frihedsrettigheder, herunder beskyttelse af personoplysninger.

Opbevaringsbegrænsning: Personoplysninger skal slettes eller gøres anonyme, når det ikke længere er nødvendigt for den dataansvarlige at have oplysningerne.

Persondatasikkerhedsbrud: Når persondata går tabt, bliver utilgængelig, tilintetgjort, ændret, kompromitteret, offentliggjort, videregivet eller på anden vis bliver tilgængeligt for uvedkommende. Det kan f.eks. være, hvis vi kommer til at sende breve til den forkerte borgers e-boks, eller hvis vores it-systemer bliver hacket.

Registrerede: Den person som personoplysningerne vedrører, f.eks. en borger, bruger eller medarbejder.

Risikovurdering: En vurdering af de potentielle risici for den registrerede, der er forbundet med behandlingen af personoplysninger. Vurderingen skal tage udgangspunkt i tre parametre: fortrolighed, tilgængelighed og integritet.