Introduktion til persondataforordning

Lektor Dorte Høilund

- Anvendelse fra 25. maj 2018
- Direktiv contra forordning
- Mange muligheder for nationale særregler
- Opbygning og struktur
- Forslag til Databeskyttelseslov

Emner

- Anvendelsesområde og centrale begreber
- Regler for behandling af personoplysninger
- Registrerede personers rettigheder
- Den nye rolle som databeskyttelsesrådgiver
- Krav til datasikkerhed
- Sanktioner

Forordningen gælder først og fremmest for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikke-automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register jf. art. 2(1).

Gælder både for offentlige myndigheder og private virksomheder

Grundlæggende principper (art. 5)

- God databehandlingsskik
- Udtrykkelige og saglige formål
- Proportionalitetsprincippet
- God datakvalitet
- Tidsbegrænsningsprincippet
- Sikkerhedsprincippet

Betingelser for behandling af personoplysninger

- Alm. personoplysninger (art. 6)
- Følsomme personoplysninger (art. 9)

Artikel 6: Almindelige personoplysninger

- Borgeren har givet sit samtykke
- Opfyldelse af en kontrakt
- Overholdelse af en retlig forpligtelse
- Beskyttelse af vitale interesser
- Samfundsinteresse eller offentlig myndighedsudøvelse
- Interesseafvejningsreglen

Artikel 9: Følsomme oplysninger

Oplysninger om:

- Race
- Politisk, religiøs eller filosofisk overbevisning
- Fagforeningsmæssigt tilhørsforhold
- Genetiske data og biometriske data
- Helbredsoplysninger (fysiske og psykiske)
- Seksuelle forhold eller seksuel orientering

Udgangspunktet er, at der ikke må behandles følsomme personoplysninger, medmindre en af undtagelserne i artikel 9(2) er tilstede.

Registrerede personers rettigheder

- Ret til at få information
- Ret til indsigt
- Ret til at få urigtige oplysninger berigtiget
- Retten til at blive glemt
- Ret til begrænsning af behandling
- Ret til dataportabilitet
- Ret til at protestere mod at behandling af oplysninger finder sted
- Ret til at protestere mod visse automatiserede individuelle afgørelser

Oplysningspligt (art. 13 og 14)

- Dataansvarliges identitet + **eventuel DPO**
- Formål + **behandlingsgrundlag**
- **Hvis interesseafvejning – angiv interesser**
- (Kategorier af) modtagere
- **Evt. tredjelandsoverførsel og hjemmel hertil**
- **Opbevaringsperiode (eller kriterier)**
- Oplyse om rettigheder
- **Ret til at tilbagekalde samtykke**
- **Klage til Datatilsynet**
- **Om afgivelsen følger af lov eller er nødvendig for at indgå en aftale**
- **Om den registrerede har pligt til at give oplysningerne og evt. konsekvenser af ikke at give oplysninger**
- **Oplysninger om behandling baseret på automatiseret afgørelse**
- **Ved indsamling hos tredjemand: typen af oplysninger, der er indsamlet, samt hvor de er indsamlet fra.**

Nyt formål kræver ny meddelelse herom

Databeskyttelsesrådgiver (DPO)

Obligatorisk for offentlige myndigheder

Stilling

- Må ikke modtage instrukser vedrørende udførelse af sine opgaver
- Må ikke afskediges eller straffes for at udføre sine opgaver
- Rapporterer direkte til den øverste ledelse
- Kan udføre andre opgaver, men der må ikke være interessekonflikt

Databeskyttelsesrådgiverens opgaver (minimumskrav):

- Underrette og rådgive om forpligtelser iht. forordningen og anden EU-ret eller national ret om databeskyttelse
- Overvåge overholdelse af forordningen, anden EU-ret eller national ret om databeskyttelse samt politikker om beskyttelse af personoplysninger, herunder fordeling af ansvar, oplysningskampagner og uddannelse af det personale, der medvirker ved behandlingsaktiviteterne
- Rådgive, når der anmodes herom, med hensyn til konsekvensanalyse vedrørende databeskyttelse og overvåge opfyldelse iht. art. 35
- Samarbejde med og fungere som kontaktperson for Datatilsynet

Indbygget databeskyttelse

Databeskyttelse gennem design

Databeskyttelse gennem standardindstillinger

Accountability

Den dataansvarlige skal kunne dokumentere at de grundlæggende principper i art. 5(1) overholdes, jf. art 5(2).

Den dataansvarlige har pligt til at gennemføre passende og effektive foranstaltninger og til at påvise, at behandling af personoplysninger overholder forordningen, jf. artikel 24(1).

Risikovurdering – sikkerhedsniveau skal passe til risici

Art. 30 - fortegnelse

Både dataansvarlig og databehandler skal fører fortegnelser over behandlingsaktiviteter under deres ansvar, jf. art 30.

Dokumentationen skal som minimum indeholde:

- Navn og kontaktinformation på dataansvarlig, og hvis relevant DPO
- Formålene med behandlingen
- Kategorier af registrerede personer og kategorierne af personoplysninger
- Kategorier af modtagere af oplysninger
- Hvis relevant: overførsler til tredjelande
- Hvis det er muligt angivelse af tidsfrister for sletning af de forskellige kategorier af oplysninger
- En generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i art. 32, stk. 1.

NB: Undtagelser i art. 30, stk. 5

Fortegnelserne skal efter anmodning stilles til rådighed for Datatilsynet

Datasikkerhed

Artikel 32

Gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til risici.

- Teknisk sikkerhed - rettet mod teknologien. Fx firewalls, backup, kryptering mv.
- Organisatorisk sikkerhed – rettet mod de personer, som foretager behandling af personoplysninger. Fx begrænsning af adgang, udd. af medarbejdere og kontrolforanstaltninger.
- Fysisk sikkerhed – Rettet mod risikoen for, at uvedkommende offline får adgang til personoplysninger. Fx aflåsning, alarmer, brandsikring mv.

Datasikkerhedsbrister

Orientering Datatilsynet (art. 33):
Anmeldelse af brud på persondatasikkerheden til Datatilsynet inden 72 timer, medmindre det er usandsynligt, at bruddet indebærer en risiko

Orientering af den registrerede (art. 34):
Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, underretter den dataansvarlige uden unødig forsinkelse den registrerede om bruddet

NB: visse undtagelser

Administrative bøder