Datatyper i GDPR og klassificering ud fra sensitivitet

Almindelige personoplysninger

Disse oplysninger kan identificere en person direkte eller indirekte. De kræver **almindelig beskyttelse**, men er stadig dækket af GDPR.

Eksempler:

- Navn
- Adresse
- Telefonnummer
- E-mail
- IP-adresse
- Brugeradfærd (cookies, tracking)
- Medarbejdernummer

Brugsscenarie: En webstore har kunderegistre med navn, leveringsadresse og e-mail. Disse data skal beskyttes, men er ikke automatisk klassificeret som følsomme.

2. Følsomme personoplysninger (særlige kategorier)

GDPR definerer særlige kategorier af data, som kræver **strengere beskyttelse**. Behandling af disse data er som udgangspunkt forbudt, medmindre der foreligger et lovligt behandlingsgrundlag.

Eksempler:

- Helbredsoplysninger
- Seksuel orientering
- Biometriske data (f.eks. fingeraftryk, ansigtsgenkendelse)
- Race eller etnisk oprindelse
- Politisk overbevisning
- Fagforeningsmedlemskab
- Religiøs overbevisning

Brugsscenarie: Et HR-system gemmer helbredsoplysninger om medarbejdere i forbindelse med sygefravær. Disse oplysninger må kun være tilgængelige for autoriseret personale og kræver både tekniske og organisatoriske sikkerhedsforanstaltninger.

Strafferetslige oplysninger

Oplysninger om straffedomme og lovovertrædelser er ikke en særskilt kategori som ovenstående, men kræver **ekstra behandlingsgrundlag** og bør beskyttes på samme niveau som følsomme oplysninger.

Pseudonymiserede og anonymiserede data

To forskellige måder at beskytte personfølsomme data, der er mange forskellige måder at opnå det på og varierende argumenter for hvad der er mest hensigtsmæssigt. I større databaser understøttes det oftest gennem enkryptering.

- **Pseudonymiserede data**: Personoplysninger, hvor identificerende felter er erstattet af pseudonymer (f.eks. ID-numre). Disse er **stadig omfattet af GDPR**, fordi de kan forbindes tilbage til en person.
- **Anonymiserede data**: Data, hvor identiteten **ikke længere kan bestemmes** (hverken direkte eller indirekte). Disse er **ikke omfattet af GDPR**.

Klassificering efter behov for fortrolighed

Organisationer bør opdele data i **klassifikationsniveauer**, f.eks.:

Klassifikation	**Eksempel**	**Krav til adgangsstyring**
Høj (følsom)	Helbredsdata, CPR-nummer	Begrænset adgang, logging, kryptering
Mellem (personlig)	Navn, adresse, e-mail	Rollebaseret adgang, adgangslogning
Lav (offentlig)	Åbent CV, virksomhedsnavn	Kan være offentlig tilgængeligt

Databehandlingsaftaler og ansvarsfordeling

Når man arbejder med personoplysninger, især på vegne af andre eller på tværs af organisatoriske enheder, er det vigtigt at forstå **hvem der er dataansvarlig**, og **hvem der er databehandler**. Dette har både **juridiske** og **praktiske** konsekvenser for, hvordan systemet og adgangsstrukturen skal designes.

Begreber

- **Dataansvarlig**: Den organisation eller person, der bestemmer formålet med og midlerne til behandlingen af personoplysninger.
- **Databehandler**: En ekstern part (ofte en it-leverandør eller samarbejdspartner), som behandler data på vegne af den dataansvarlige.

Praktiske overvejelser

Hvis jeres database eksempelvis hostes i skyen, skal I tage stilling til, **hvem der opbevarer og tilgår data**, og **hvem der har ansvaret for sikkerheden**.

- I tilfælde hvor I udarbejder en prototype eller demo til en kunde, skal det også fremgå, **hvilke roller i systemet opererer som databehandlere**, og hvordan deres adgang er begrænset i overensstemmelse med GDPR.

Databehandleraftaler

I skal derfor overveje, hvordan databehandleraftaler kunne se ud i jeres løsning:

- Hvilke datatyper må databehandleren tilgå?
- Skal der være tekniske begrænsninger (f.eks. read-only adgang)?
- Hvordan dokumenteres det, at man overholder disse begrænsninger?

Eksempel:
Et analysefirma, der hjælper en webshop med forretningsindsigt, er databehandler. De må kun tilgå anonyme eller pseudonymiserede data om kundeadfærd – ikke direkte identificerbare oplysninger som navn, e-mail og betalingsoplysninger. Det skal afspejles både i datamodellen og adgangsstrukturen.