**Skabelon til konsekvensanalyse**

**Databeskyttelsesforordningen stiller som noget nyt krav om, at man i visse situationer skal foretage en konsekvensanalyse eller en såkaldt DPIA (Data Protection Impact Assessment).**

Hvis man foretager databehandling der, f.eks. ved brug af nye teknologier og pga. sin karakter, omfang og formål, sandsynligvis vil indebære en høj risiko for personers rettigheder og frihedsrettigheder, så skal man nok udarbejde en konsekvensanalyse.

En konsekvensanalyse vil typisk også være påkrævet, hvis man behandler følsomme oplysninger i stort omfang, eller hvis man beskæftiger sig med profilering og systematisk overvågning af offentligt tilgængelige områder.

**Skal der laves en konsekvensanalyse?**

For at vurdere, om man overhovedet skal lave en konsekvensanalyse, anbefaler EU at man kigger på følgende kriterier:

1. **Indsamles data med henblik på evaluering eller scoring?**
F.eks. data om en persons performance på arbejdet, økonomiske situation, helbred, personlige interesser eller opførsel.
2. **Benyttes data til automatiserede beslutninger, der har juridisk effekt?**Det kan være maskinbeslutninger, der ender med at ekskludere eller diskriminere enkeltpersoner. F.eks. hvis en softwarerobot afgør, at en bestemt person ikke kan få en forsikring eller offentlig ydelse.
3. **Foretages der systematisk overvågning?**Hvis man systematisk overvåger offentlige områder, som f.eks. nummerpladegenkendelse i et parkeringshus. Det kan også være virksomheder, der overvåger medarbejdernes brug af pc’er og internetaktivitet.
4. **Indsamles følsomme data?**Hvis man f.eks. behandler data om folks politiske holdninger, deres straffeattest, lokationsdata og patientdata.
5. **Behandles store mængder data (Big Data)?**Persondataforordningen har ikke defineret, hvornår der er tale om databehandling i stor skala, så det er pt. op til virksomheden selv at vurdere.
6. **Sammenkobles datasæt der giver ny viden?**F.eks. to datasæt der er indsamlet med hvert sit formål og så sat sammen for at give ny indsigt om en specifik person. Et eksempel kunne være en virksomhed, der havde et datasæt om personers madvaner og et datasæt om deres motionsvaner, men som kombineret giver en ny detaljeret sundhedsprofil.
7. **Vedrører data udsatte personer?**
Det kan være data om børn, mentalt syge, asylsøgere, ældre eller patienter.
8. **Anvendes ny teknologi?**
Hvis man i sine løsninger bruger ny teknologi som f.eks. fingeraftrykslæsere, ansigtsgenkendelse eller IoT-produkter, kan en DPIA være nødvendig.
9. **Bliver data overført udenfor EU.**
Hvis ens data er placeret uden for EU’s grænser, og i lande der [ikke er godkendt af EU](https://itb.dk/raadgivning/vaerktoejer/persondataforordningen/overfoersel-til-tredjelande/).
10. **Har personen ingen mulighed for at sige nej.**
Det kan f.eks. være overvågning af områder, hvor folk der blot passerer forbi ikke kan undgå at blive registreret, eller hvis en bank automatisk laver en kreditvurdering, der i sidste ende kan gøre, at personen ikke får adgang til en service eller kontrakt.

Kan du sige ja til en eller flere af ovenstående, skal I som udgangspunkt lave en konsekvensanalyse eller som minimum skrive ned, hvorfor I har valgt ikke at lave en.

**Det skal en konsekvensanalyse indeholde**
Hvilken metode, man vil bruge i forbindelse med at udarbejde en konsekvensanalyse, står en frit for selv at vælge.

[Datatilsynet i Danmark skriver](https://www.datatilsynet.dk/media/6866/12-spoergsmaal-om-forordningen.pdf) dog følgende: Konsekvensanalysen skal bl.a. omfatte en systematisk beskrivelse af de planlagte behandlingsaktiviteter, en vurdering af behandlingsaktiviteternes nødvendighed og rimelige forhold til formålene, en vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder og en beskrivelse af de foranstaltninger, der påtænkes med henblik på at imødegå de konstaterede risici.

Du kan bruge denne template som udgangspunkt til at udarbejde en DPIA.

|  |  |
| --- | --- |
| Navn på plan: | Ansvarlig: |
| Dato for udførelse: | Dato for forventet afslutning: |
| **Beskrivelse af dataprocessen:**Beskrivelsen skal indeholde baggrunden og formålet med dataindsamlingen. Besvar følgende spørgsmål:1. Hvilke oplysninger er det, som du indsamler eller behandler, og kan enkeltpersoner blive identificeret ud fra disse oplysninger (f.eks. personnavne, adresser, helbredsoplysninger, IP-adresser, e-mail adresser, etc.)?
2. Hvad er formålet med at behandle disse data (et eksempel kunne være, at man opbevarer kundeoplysninger så man kan fakturere sine kunder.), og er personoplysningerne nødvendige for at kunne opfylde formålet?
3. Hvad vil I gøre med disse data (Vil der eksempelvis ske en registrering, redigering, sammenstilling, videregivelse, osv.) – og hvad sker der med dem, når I er færdige med databehandlingen?
 |
| **Analyse af risiko:**Beskriv hvilke risiko der er, hvor alvorlige de er, og hvor hvilken indvirkning de har på de pågældende personer. Indsamler og behandler man persondata i forhold til de 10 punkter nævnt i ovenstående, og er der en høj risiko, så skal det skrives som årsag til at lave en konsekvensanalyse.1. Er der risiko for, at disse data på et tidspunkt vil blive brugt til noget andet, end det de oprindeligt var indsamlet til (f.eks. til udsending af reklame) og vil det kunne skade personerne, hvis uvedkommende fik fat i deres data (økonomisk, fysisk, renommemæssig eller lignende skade)?
2. Hvem har adgang til disse data (hvem kan se dem, og hvem kan rette i dem) og er der risiko for, at disse data kan falde i uvedkommendes hænder (f.eks. ved at de bliver sendt ukrypteret via mail eller at uvedkommende personer har adgang til data)?
3. Hvordan bliver data opbevaret (f.eks. i et fysisk i et arkiv, på et kontor, i en computer eller i skyen (cloud computing), og er teknologien designet til at kunne håndtere persondata (e-Boks er f.eks., mens et Excel-ark ikke er)? Er teknologien sikkerhedstestet, og hvor tit sker dette?
4. Kan der ved uheld ske ændringer i data (kan de f.eks. blive slettet eller ændret ved en fejl)?
 |
| **Modforanstaltninger:**For hver risiko, skal man beskrive, hvad virksomheden konkret gør for at minimere risikoen – og hvad virksomheden vil gøre, hvis uheldet alligevel er ude. |
| **Skal Datatilsynet kontaktes:** Ja/nejHusk at hvis virksomheden vurderer, at risikoen er særlig høj, skal Datatilsynet også underrettes. |

Du kan altid få hjælp og finde svar på vores [temaside om persondataforordningen](https://itb.dk/raadgivning/vaerktoejer/persondataforordningen/).

Er du interesseret Databeskyttelse og Privacy generelt, skal du måske være med i [IT-Branchens it-sikkerhedsudvalg](https://itb.dk/voresudvalg/it-sikkerhed/). Kontakt Martin Jensen Buch, mjb@itb.dk, hvis du vil høre mere om, hvad udvalget laver.