VEJLEDNING

KONSEKVENSANALYSE

**Hvad er en konsekvensanalyse?**

En konsekvensanalyse er en analyse af de konsekvenser, som en given behandlingsaktivitet vil have for beskyttelsen af de pågældende personoplysninger.

Analysen har det formål at skulle vurdere de risici, som er forbundet med en given behandling af personoplysninger, med henblik på at forebygge brud på persondatasikkerheden. Det skal dog bemærkes, at der er tale om risici for den registrerede og ikke risici for selve virksomheden eller organisationen.

Konsekvensanalysen skal foretages således, at en den dataansvarlige tvinges til at overveje de negative konsekvenser, som en given behandling kunne have.

Datatilsynet har opstillet en række skridt, som skal foretages i forbindelse med udarbejdelse af en konsekvensanalyse:

1. Der skal foretages en vurdering af, hvorvidt den pågældende type af persondatabehandling vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
2. Hvis dette er tilfældet, så foretages en konsekvensanalyse
3. Denne konsekvensanalyse skal udarbejdes med udgangspunkt i at træffe passende foranstaltninger til at begrænse de risici, som er angivet i konsekvensanalysen, og overholde Databeskyttelsesforordningens krav
4. Hvis det ikke findes muligt at begrænse de påviste risici, skal man som dataansvarlig kontakte Datatilsynet, inden den planlagte behandling igangsættes

Det er ikke et krav efter forordningen, at konsekvensanalysen offentliggøres. Den dataansvarlige kan dog vælge at offentliggøre konsekvensanalysen, da dette vil kunne bidrage til at skabe gennemsigtighed.

**Hvornår skal der foretages en konsekvensanalyse?**

Man er som dataansvarlig alene forpligtiget til at lave en konsekvensanalyse, hvis det er sandsynligt, at der foreligger en høj risiko for fysiske personers rettigheder og frihedsrettigheder forbundet med behandlingen af oplysninger. Der er her tale om risici forbundet med den registreredes rettigheder, og ikke risici forbundet med selve organisationen eller virksomheden.

Udgangspunktet er altså, at når en behandling af personoplysninger formodentlig vil kunne medføre en høj risiko for en fysisk persons persondatarettigheder, skal den dataansvarlige udarbejde en konsekvensanalyse.

Forordningen kræver, at den pågældende konsekvensanalyse iværksættes inden behandlingen af persondata påbegyndes. Dernæst kræves det, at en eventuel databeskyttelsesrådgiver skal inddrages og yde rådgivning i forbindelse med udarbejdelsen af selve konsekvensanalysen.

Vejledende momenter i bedømmelsen af, om en konsekvensanalyse skal foretages:

* Det vil være relevant at kigge på, om den pågældende behandling benytter **nye teknologier** eller anvender teknologier på nye måder. Hvis dette er tilfældet, vil det tyde på, at der bør foretages en konsekvensanalyse, da konsekvenserne ved anvendelsen af sådanne nye teknologier kan afdække ubekendte faktorer.
  + Nye teknologier omhandler teknologier, der på grund af deres nyhedsværdi kun har eksisteret i relativt kort tid eller aldrig har været i brug. Hvis man som dataansvarlig udskifter sin IT-platform, betyder det ikke, at der er tale om en ny teknologi. Hvorvidt der er tale om ny teknologi afhænger af niveauet af den teknologiske viden, der er opnået.
* Det kan være relevant at kigge på, om behandlingen af personoplysningerne kan føre til fysisk, materiel eller immateriel skade. Dette forekommer hvis:
  + Behandlingen kan give anledning til at der udvises forskelsbehandling, skade på omdømme, tab af fortrolighed for personoplysninger, som er omfattet af tavshedspligten, finansielle tab, identitetstyveri, uautoriseret ophævelse af pseudonymisering, svig eller andre økonomiske eller sociale konsekvenser
  + De registrerede kan fratages deres rettigheder eller forhindres i at føre kontrol med deres personoplysninger
  + De personoplysninger der behandles falder inden for kategorien af de følsomme oplysninger
  + Personlige forhold evalueres som et led i behandlingen af disse oplysninger
  + Personoplysninger behandles om fysiske personer, som er sårbare. Sårbare registrerede vil hovedsageligt omhandle børn eller registrerede med behov for særlig beskyttelse, såsom psykisk syge, asylansøgere m.v.
* Hvis der foretages systematisk og omfattende vurdering af personlige forhold baseret på automatisk behandling, så er det formentlig påkrævet at lave en konsekvensanalyse.
* Hvis der foretages behandling af følsomme oplysninger i et stort omfang, bør en konsekvensanalyse udarbejdes. Når det skal vurderes om der er tale om behandling i et ”stort omfang”, er det relevant at se på:
  + Antallet af fysiske personer, der behandles personoplysninger om
  + Mængden af personoplysninger som bliver behandlet, samt mængden af de forskellige typer af personoplysninger, som der foretages behandling omkring
  + Hvor lang tidsperioden for behandlingen er, og eventuelt om behandlingen er permanent
  + Det geografiske omfang af behandlingsaktiviteterne
* Hvis der foretages overvågning af et offentligt tilgængeligt område i stort omfang, vil en konsekvensanalyse sandsynligvis være påkrævet. Her skal vurderingen af, hvorvidt der er tale om ”stort omfang” foretages (se forrige punkt).

**En fælles konsekvensanalyse?**

Det er med Databeskyttelsesforordningen gjort muligt at foretage en fælles konsekvensanalyse for flere behandlingsaktiviteter. Dette er dog kun muligt, hvis der er tale om lignende behandlingsaktiviteter, som indebærer lignende høje risici.

Dette kan være relevant, hvis der er flere dataansvarlige, som i samarbejde planlægger en behandling af personoplysninger. Førend, at man kan gå sammen om at lave en fælles konsekvensanalyse, skal der være tale om samme type af system, den samme behandlingsaktivitet af samme former for personoplysninger, og at behandlingsaktiviteterne indebærer samme høje risici. Det er ikke et krav, at systemerne og behandlingsaktiviteterne er fuldstændig identiske, men disse må ikke adskille sig væsentligt fra hinanden.

Det er de dataansvarlige selv, som står for at skulle anslå om henholdsvis systemerne og behandlingsaktiviteterne er identiske.

Når man som dataansvarlig foretager en fælles konsekvensanalyse sammen med andre dataansvarlige, er de enkelte dataansvarlige selv forpligtiget til at udarbejde en fortegnelse af konsekvensanalysen. Det er derfor også den enkelte dataansvarlige, der er ansvarlig for sin egen fortegnelse heraf.

**Indholdet af en konsekvensanalyse**

Som minimum skal konsekvensanalysen indbefatte følgende:

* En beskrivelse af de påtænkte behandlingsaktiviteter. Formålene med denne behandling, og deriblandt de legitime interesser, som efterstræbes af den dataansvarlige, skal ligeledes indgå i beskrivelsen.
* En vurdering af, hvorvidt de påtænkte behandlingsaktiviteter er fornødne, samt om disse står i et rimeligt forhold til formålene med behandlingen, skal foretages. Det opstillede krav skal forebygge en samling af data, samt skal dette krav sikre, at behandlingen af personoplysningerne kun sker på det grundlag, at de er nødvendige og er i overensstemmelse med formålene med behandlingen.
* En vurdering af risiciene for de registreredes rettigheder samt frihedsrettigheder. Dette betyder, at risiciene ved den registreredes rettigheder skal anslås i forhold til den påtænkte behandling og formålet med behandlingen.
* Herudover skal de foranstaltninger, der planlægges for at imødekomme disse risici, vurderes. Dette drejer sig om blandt andet sikkerhedsforanstaltninger, garantier og mekanismer, der både kan sikre overholdelse af Databeskyttelsesforordningen og beskyttelsen af personoplysningerne. Der skal altså iværksættes en vurdering af, hvilke foranstaltninger, man har tænkt sig at indføre, for at imødekomme de risici, som ved tidligere konstateringer stadig foreligger. Her skal man huske på, at der formentlig kræves forskellige foranstaltninger til forskellige typer af risici.

**Undtagelse fra pligten til at foretage konsekvensanalyse**

Hvis persondatabehandlingen er nødvendig for at overholde en retlig forpligtigelse, er den dataansvarlige undtaget fra pligten til at foretage en konsekvensanalyse.

Det samme gælder, hvis behandlingen er nødvendig af hensyn til udførelse af en konkret opgave, der er i samfundets interesse eller som varetages af offentlig myndighedsudøvelse.

**Hvornår skal konsekvensanalysen fornys?**

Hvis der sker ændringer, som kan påvirke de vurderede risici, skal der foretages en ny gennemgang af behandlingsaktiviteterne for at vurdere, om behandlingen fortsat foretages i overensstemmelse med konsekvensanalysen.

Ligeledes skal konsekvensanalysen gennemgås, hvis formålet med behandlingerne forandres eller hvis der fremover skal behandles andre typer af personoplysninger.

**Forudgående høring af Datatilsynet**

Der er, som tidligere nævnt, visse behandlinger som kræver, at tilsynsmyndigheden skal høres forud for behandlingens start.

Tilsynsmyndigheden skal høres inden behandlingen, hvis konsekvensanalysen påviser, at behandlingen vil medføre en høj risiko, og den dataansvarlige ikke har mulighed for at indføre passende foranstaltninger, der har til formål at begrænse disse risici.