DATATILSYNET

JUSTITSMINISTERIET

Konsekvensanalyse

Marts 2018

Indhold

1. Forord

Denne vejledning er primært skrevet til dig, der som *dataansvarlig*[1] har brug for hjælp til at vide, hvornår du skal foretage en konsekvensanalyse vedrørende databeskyttelse.

Når du som privat virksomhed, offentlig myndighed, fysisk person, institution eller ethvert andet organ har ansvaret for en behandling (f.eks. indsamling, registrering, videregivelse eller sletning) af personoplysninger om andre personer, er det vigtigt at være opmærksom på, at du i tilstrækkelig grad beskytter de oplysninger, du har ansvaret for behandlingen af. Det er i den forbindelse et krav, at du som dataansvarlig gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at din behandling er i overensstemmelse med databeskyttelsesforordningen.

Derfor skal du som dataansvarlig vurdere, hvilke negative konsekvenser en behandling vil kunne få. På denne måde kan du på et oplyst grundlag tage stilling til, om behandlingen – på trods af de risici der er identificeret herved – skal påbegyndes.

Med databeskyttelsesforordningen afskaffes den generelle anmeldelsespligt til Datatilsynet. I stedet skal der nu bl.a. foretages en konsekvensanalyse vedrørende databeskyttelse, når der sandsynligvis er en høj risiko for, at behandlingen af oplysninger kan krænke den registreredes rettigheder og frihedsrettigheder med henblik på at fastsætte foranstaltninger til at imødegå disse risici. Dette vil være med til at skabe bedre databeskyttelse og hænger sammen med forordningens røde tråd om ansvarlighed.

Konsekvensanalysen kan hjælpe dig til at identificere og begrænse de påviste risici ved en given behandling. Resultatet af konsekvensanalysen bør således tages i betragtning, når der skal træffes passende foranstaltninger med henblik på at påvise, at behandlingen af personoplysninger overholder de databeskyttelsesretlige regler.

Formålet med databeskyttelsesforordningens regler om konsekvensanalyser er at indramme og koncentrere sig om den behandling af oplysninger, som faktisk medfører væsentlige risici for de registrerede fremfor at anmelde al persondatabehandling til Datatilsynet. Konsekvensanalysen er et centralt element i overholdelsen af databeskyttelsesforordningen, når der planlægges eller foretages databehandling med høj risiko.

Der henvises i øvrigt til Artikel 29-gruppens vejledning om ”Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen ”sandsynligvis indebærer en høj risiko” i henhold til forordning (EU) 2016/679”[2].

[1] Se *vejledning om dataansvarlige og databehandlere* for en nærmere gennemgang af hvornår man er dataansvarlig: https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_om_dataansvarlige_og_databehandlere_-_endelig_version.pdf.

[2] Du kan på Datatilsynets hjemmeside: www.datatilsynet.dk, finde et direkte link til vejledningen på dansk.

2. Hvad er en konsekvensanalyse?

En konsekvensanalyse vedrørende databeskyttelse (data protection impact assessment) er, som navnet antyder, en analyse af påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger.

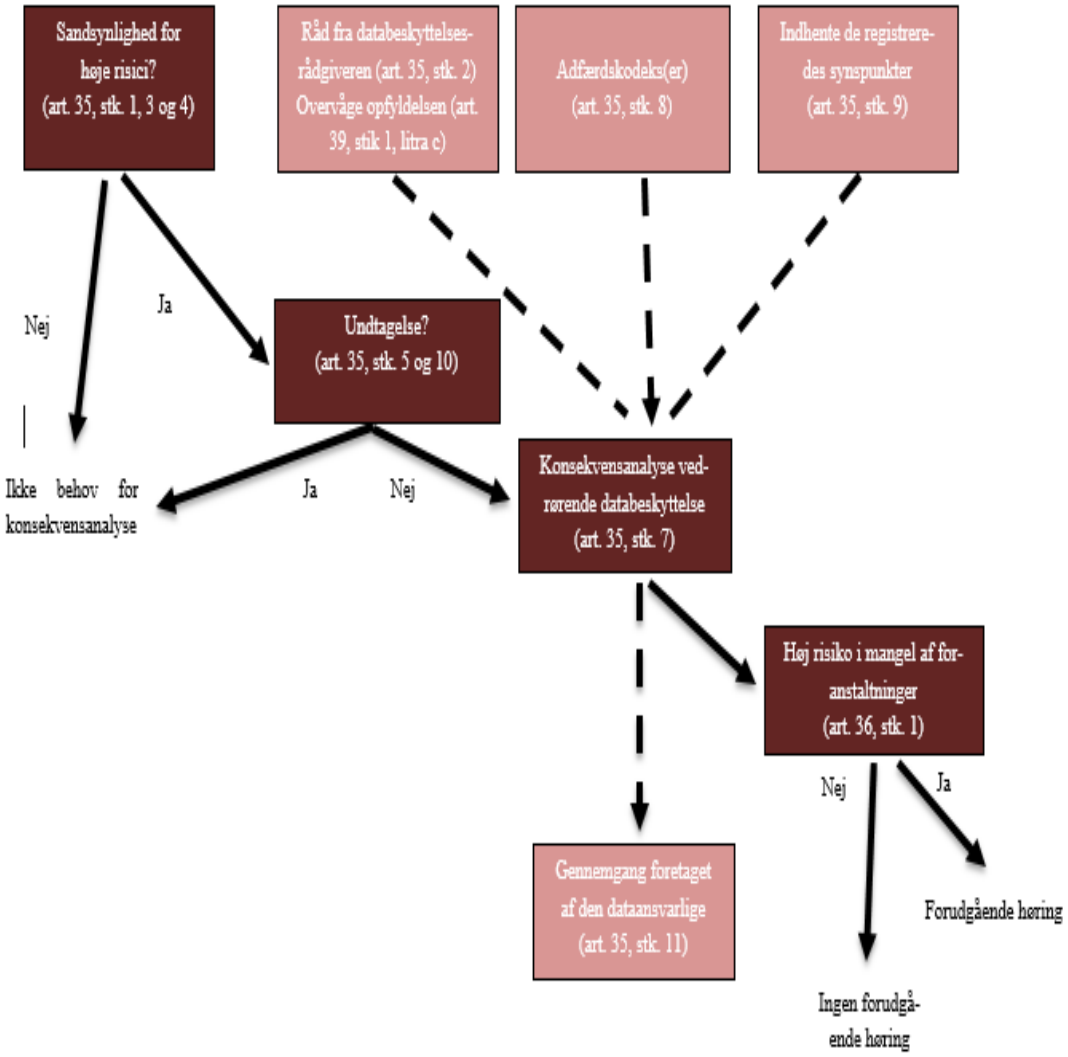
Det er en proces – herunder et sæt af konkrete produkter, som skabes ved processen – der har til formål at vurderer risici for fysiske personers rettigheder og frihedsrettigheder og fastlægge foranstaltninger til at afhjælpe disse risici. Analysen skal således beskrive, hvilken behandling der foretages, vurdere behandlingens nødvendighed og proportionalitet og bidrage til at håndtere de risici, som behandlingen af personoplysninger medfører.

Du har som dataansvarlig alene 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. Har du konstateret, at der sandsynligvis er en høj risiko, er det ligeledes dig, der har ansvaret for at foretage en konsekvensanalyse. Foretages en behandling af en databehandler, skal denne hjælpe dig som dataansvarlig med at udføre konsekvensanalysen. Databehandleren skal endvidere sørge for at give dig den nødvendige information for at gennemføre analysen. Risikovurderingen angår således risici for den registrerede og ikke organisationens (f.eks. en virksomheds) risici.

Det følger endvidere af forordningen, at du skal rådføre dig med din databeskyttelsesrådgiver, hvis du har en, når der foretages en konsekvensanalyse.

Grundlæggende skal du igennem følgende skridt i forbindelse med en konsekvensanalyse vedrørende databeskyttelse **1)** foretage en vurdering af, hvorvidt en type behandling sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder. Er dette tilfældet **2)** foretager du en konsekvensanalyse vedrørende databeskyttelse med henblik på **3)** at træffe passende foranstaltninger til at begrænse de påviste risici ved behandlingen og overholde forordningens krav. Er det ikke muligt at begrænse de påviste risici ved passende foranstaltninger, således at risikoen fortsat er høj skal du **4)** høre Datatilsynet forud for igangsættelse af den påtænkte behandling.

Det er ikke et krav, at man offentliggør en konsekvensanalyse vedrørende databeskyttelse. Det er den dataansvarliges beslutning, om dette skal ske. En offentliggørelse kan dog være med til at skabe bedre gennemsigtighed. Fremfor at offentliggøre hele din konsekvensanalyse, kan en offentliggørelse bestå af f.eks. et ledelsesresumé.


Sandsynlighed for høje risici? (art. 35, stk. 1, 3 og 4)
Råd fra databeskyttelses-rådgiveren (art. 35, stk. 2) Overvåge opfyldelsen (art. 39, stik 1, litra c)
Adfærdskodeks(er) (art. 35, stk. 8)
Indhente de registrere-des synspunkter (art. 35, stk. 9)
Nej
Ja
Undtagelse? (art. 35, stk. 5 og 10)
Ikke behov for konsekvensanalyse
Ja
Nej
Konsekvensanalyse ved-rørende databeskyttelse (art. 35, stk. 7)
Høj risiko i mangel af for-anstaltninger (art. 36, stk. 1)
Nej
Ja
Gennemgang foretaget af den dataansvarlige (art. 35, stk. 11)
Forudgående høring
Ingen forudgå-ende høring

3. Hvornår skal den dataansvarlige foretage en konsekvensanalyse?

Hvad siger forordningen:

Det fastsættes generelt i databeskyttelsesforordningens artikel 35, stk. 1, 1. pkt., hvornår den dataansvarlige skal foretage en konsekvensanalyse:

"*Hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, foretager den dataansvarlige forud for behandlingen en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger*."

Med databeskyttelsesforordningen indføres således et udgangspunkt om, at du som dataansvarlig skal gennemføre en konsekvensanalyse, når en behandling sandsynligvis vil indebære en høj risiko for, at den person, der behandles oplysninger om, får krænket sine rettigheder og frihedsrettigheder.

En sådan konsekvensanalyse skal foretages, *inden* du påbegynder behandlingen, jf. i øvrigt punkt 3.3. om eksisterende behandlingsaktiviteter.

Det bemærkes i øvrigt, at du skal rådføre dig med din databeskyttelsesrådgiver – hvis din organisation har udpeget en – når der foretages en konsekvensanalyse vedrørende databeskyttelse.

3.1. Nye teknologier

Når du som dataansvarlig skal vurdere, om en type behandling sandsynligvis vil medføre en høj risiko for krænkelser af en fysisk persons rettigheder og frihedsrettigheder, som dermed kræver, at du foretager en konsekvensanalyse, er det navnlig relevant at se på, om behandlingen gør brug af *nye teknologier*, herunder også anvendelse af teknologier på en ny måde. At det navnlig er ved anvendelse af nye teknologier skyldes, at brug af ny teknologi kan indebære nye former for dataindsamling og – anvendelse, eventuelt med en høj risiko for fysiske personers rettigheder og frihedsrettigheder. De personlige og sociale konsekvenser af ibrugtagningen af ny teknologi kan være ukendte (f.eks. for borgernes dagligdag eller privatlivets fred). En konsekvensanalyse vil således hjælpe dig med at forstå og behandle disse risici.

Der skal objektivt set være tale om ny teknologi. Hvis du som dataansvarlig har udskiftet din IT-platform, betyder det ikke, at der objektivt set er tale om ny teknologi. Du har måske blot konkret fået et nyt IT-system, som dog ikke udgør en "ny teknologi". Det er dog vigtigt at være opmærksom på, at der – henset til at det "navnlig" vil være ved brug af nye teknologier – fortsat kan være behov for at skulle udarbejde en konsekvensanalyse, selvom der ikke konkret er tale om en "ny teknologi".

Vurderingen af, om der er tale om ny teknologi, skal i øvrigt ske i overensstemmelse med det opnåede niveau af teknologisk viden.

Eksempel
Som eksempel på "nye teknologier" kan nævnes brugen af biometrisk data. Biometri er den samlede betegnelse for en række teknikker til identifikation og genkendelse af personer ved hjælp af unikke biologiske kendetegn hos personerne. De biometriske teknikker bygger f.eks. på elektronisk genkendelse af ansigt, øjne, fingre, stemme, hænder, vener og gangart. Der er ikke nødvendigvis tale om ny teknologi blot fordi, der anvendes biometriske oplysninger, men biometriske teknikker vil kunne indgå i ny teknologi, ligesom eksisterende biometrisk teknologi efter omstændighederne kan blive anset for ny teknologi, f.eks. hvis det anvendes på en ny måde.

Eksempel
Et andet eksempel på "ny teknologi" er politiets anvendelse af automatisk nummerpladegenkendelse (ANPG). Systemet – der dog ikke er omfattet af databeskyttelsesforordningen, men af retshåndhævelsesdirektivet – består af en række stationære kameraer opstillet ved vejstrækninger og mobile kameraer fastsat på f.eks. patruljevogne. Kameraerne genkender og læser nummerpladerne på alle biler, der passerer. På baggrund af disse læsninger kan systemet bl.a. alarmere politiet, hvis et køretøj, som er registreret på særlige "hot-lister", passerer et kamera. Bogstaver og tal i nummerpladen bliver således automatisk omsat til tekst og slået op i en database, og hvis køretøjet er kendt i de tilkoblede systemer, kommer der en besked op på skærmen i patruljevognen.

ANPG-teknologi er endvidere i de senere år blevet udbredt i den private sektor, f.eks. som led i opkrævning af betaling for parkering i p-huse mv.

Eksempel
Et andet eksempel på "ny teknologi" kan være det, der på engelsk kaldes *Internet of Things*. (på dansk: Tingenes Internet), som overordnet dækker over det fænomen, at ikke kun mennesker men også *noget*/vores *ting* bliver brugere af internettet. Det kan f.eks. være, at låsene/adgangskontrollen i din organisation registrerer, hvilke medarbejdere der går ind og ud og hvornår med henblik på f.eks. at registrere medarbejdernes arbejdstid. Det kan også tænkes anvendt med henblik på at registrere, hvornår den sidste person har forladt en bygning, så der f.eks. kan sendes information til tyverialarmen om at blive slået til eller til termostaterne i bygning om at blive slukket. Det kan også kan tænkes anvendt i forhold til at sende besked til den enkelte medarbejdes computer om at tænde, når medarbejderen møder ind.

Et andet eksempel på Internet of Things er intelligente trafiksystemer. De kan f.eks. bruges til at opkræve penge for parkering eller for at køre på gaden (road pricing) eller over en bro.

I forhold til anvendelse af teknologier på en ny måde, er det relevant at se på, om der er tale om innovativ brug af teknologi eller nye organisatoriske løsninger. Et *eksempel* herpå kan være at kombinere brugen af fingeraftryk og ansigtsgenkendelse med henblik på bedre kontrol med f.eks. fysisk adgang til visse områder.

I forbindelse med brugen af ny teknologi kan det endvidere være relevant at se på *kategorien* af de personoplysninger, der behandles. Hvis der er tale om en behandlingsaktivitet, som bruger ny teknologi, der skal behandle følsomme personoplysninger, bør der udarbejdes en konsekvensanalyse. Et eksempel på anvendelse af ny teknologi i denne situation kan være, når kunstig intelligens anvendes til at diagnosticere patienter og efterfølgende anbefale en behandling.

Eksempler på anvendelse af "nye teknologier":

- **Iris-scanning**
- **Kunstig intelligens**
- **Kommunikation med f.eks. det offentlige via apps på mobile enheder**
- **Brug af elektroniske identiteter**
- **ANPG-teknologi som led i opkrævning af parkeringsafgifter**

Brug af ny teknologi er dog ikke et krav. Vælger du f.eks. at udskifte din IT-platform, uden der er tale om brug af ny teknologi, skal du stadig vurdere, om behandlingen medfører de nævnte risici for fysiske personers rettigheder og frihedsrettigheder.

3.2. Høj risiko for fysiske personers rettigheder og frihedsrettigheder

Du har som dataansvarlig alene en pligt til at foretage en konsekvensanalyse, når der *sandsynligvis* vil være en *høj risiko* for fysiske personers rettigheder og frihedsrettigheder.

Risiciene for fysiske personers rettigheder og frihedsrettigheder kan opstå som følge af behandling af personoplysninger, der kan føre til fysisk, materiel eller immateriel skade. Det vil navnlig være tilfældet, hvis:

- Behandlingen kan give anledning til forskelsbehandling, identitetstyveri eller -svig, finansielle tab, skade på omdømme, tab af fortrolighed for personoplysninger, der er omfattet af tavshedspligt, uautoriseret ophævelse af pseudonymisering eller andre betydelige økonomiske eller sociale konsekvenser,

- De registrerede kan blive berøvet deres rettigheder og frihedsrettigheder eller forhindret i at udøve kontrol med deres personoplysninger. Den registrerede kan være hindret i at udøve en rettighed eller gøre brug af en tjeneste eller en kontrakt, hvis behandlingsaktiviteterne sigter mod at tillade, ændre eller afvise de registreredes adgang til en tjeneste eller kontrakt. Det gælder f.eks., hvis en bank screener sine kunder i forhold til en referencedatabase med henblik på at beslutte, om de skal tilbydes et lån,

- Der behandles personoplysninger, der viser race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, og behandling af genetiske data, helbredsoplysninger eller oplysninger om seksuelle forhold eller straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger,

- Personlige forhold evalueres, navnlig analyse eller forudsigelse af forhold vedrørende indsats på arbejdspladsen, økonomisk situation, helbred, personlige præferencer eller interesser, pålidelighed eller adfærd eller geografisk position eller bevægelser, med henblik på at oprette eller anvende personlige profiler,

- Der behandles personoplysninger om sårbare fysiske personer. Behandling af sådanne oplysninger er medtaget på grund af den øgede skævhed mellem den registrerede og den dataansvarlige, hvilket

betyder, at enkeltpersoner kan være ude af stand til på en nem måde at give deres samtykke til eller modsætte sig behandlingen af deres oplysninger eller udøve deres rettigheder. Sårbare registrerede omfatter navnlig børn. Det kan endvidere være mere sårbare udsnit af befolkningen med behov for særlig beskyttelse (psykisk syge personer, asylansøgere m.v.). Det kan også være tilfælde, hvor der kan konstateres ubalance mellem den registreredes og din position som dataansvarlig.

Eksempel – hvordan kan opgaven (vurdering af risici) gribes an
Når du skal vurdere, om en risiko er høj, kan det være en hjælp at starte med at identificere, hvilke risici der i det hele taget foreligger ved den påtænkte behandling. Det er i den henseende en fordel, at du gør dig overvejelser om, hvordan behandlingen skal foretages, hvilke midler der skal anvendes, samt hvilken kontekst behandlingen skal foregå i.

Helt konkret kan det bl.a. være relevant, at du får klarlagt følgende:

- Hvilke systemer skal anvendes til din behandling – er det ny teknologi?
- Hvem – og hvor mange/i hvor stort omfang – skal der behandles oplysninger om (børn, psykisk syge eller andet)?
- Hvilke oplysninger skal der behandles (følsomme)?
- Hvordan skal oplysningerne behandles (videregivelse, samkøring m.v.)?
- Hvad er formålet med behandlingen?
- Hvordan fungerer systemet, der skal foretage behandlingen (er der nogle indbyggede sikkerhedsforanstaltninger m.v. i systemet)?

Ovenstående er blot angivet som forslag til, hvilke spørgsmål du kan tage udgangspunk i, når du skal finde ud af, om du skal udarbejde en konsekvensanalyse. Når du har taget stilling til ovenstående – i kombination med eventuelle flere udredninger af relevans for din organisation – kan du tage udgangspunkt heri, når du skal søge at identificere, hvilke og hvor store risici behandlingen udgør for fysiske personers rettigheder og frihedsrettigheder (de registrerede).

Du bør bestemme risikoens sandsynlighed og alvor under hensyn til behandlingens karakter, omfang, sammenhæng og formål (er der tale om omfattende behandling, er det følsomme oplysninger, og hvad er formålet med behandlingen). Du skal evaluere risikoen på baggrund af en objektiv vurdering. I forhold til at skulle vurdere om en identificeret risiko må anses for at være høj, bør du se på mængden af data, du behandler og vurdere den i forhold til den valgte behandlingsaktivitet (f.eks. om der er tale om et stort antal personoplysninger, som skal behandles ved samstilling eller samkøring).

Der henvises nærmere til afsnit 4.1–4.3 umiddelbart nedenfor om særligt påkrævede tilfælde, hvor en behandling sandsynligvis vil indebære *høj risiko*.

3.3. Eksisterende behandlingsaktiviteter

Det er relevant at vide, i hvilket omfang, der skal foretages konsekvensanalyser for allerede igangværende behandlingsaktiviteter, når databeskyttelsesforordningen får virkning.

En konsekvensanalyse er således ikke nødvendigt for behandlingsaktiviteter, der kontrolleres af Datatilsynet i medfør af den gældende persondatalovs regler om anmeldelsespligt i kapitel 12 og 13. Har du således f.eks. foretaget en anmeldelse af din behandling i henhold til persondatalovens § 43 er behandlingen underlagt Datatilsynets kontrol, hvorfor der som udgangspunkt ikke skal udarbejdes en konsekvensanalyse. Dette gælder dog kun i det omfang, at behandlingen ikke er ændret siden anmeldelsen til Datatilsynet af behandlingen.

Er der således sket en ændring af behandlingen (i f.eks. omfang, formål, kategorien af indsamlede oplysninger, opbevaringsperiode m.v.), skal du tage stilling til, om der på baggrund af forordningens regler herom skal foretages en konsekvensanalyse, inden du påbegynder den planlagte (nye) behandlingsaktivitet.

4. Særligt påkrævede tilfælde

I dette afsnit opregnes en række ikke-udtømmende tilfælde, hvor det vil være særlig relevant for dig som dataansvarlig at foretage en konsekvensanalyse, da der vurderes at være tale om en behandling, som sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

Særligt påkrævede tilfælde

Ifølge forordningens artikel 35, stk. 3, er en konsekvensanalyse navnlig påkrævet hvis der sker:

1) en systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk behandling, herunder profilering, og som er grundlag for afgørelser, der har retsvirkning for den fysiske person eller på tilsvarende vis betydeligt påvirker den fysiske person,

2) behandling i stort omfang af særlige kategorier af følsomme personoplysninger[1] eller af personoplysninger vedrørende straffedomme og lovovertrædelser[1] eller

3) systematisk overvågning af et offentligt tilgængeligt område i stort omfang.

4.1. Systematisk og omfattende vurdering af personlige forhold baseret på automatisk behandling

Der vil være tale om et særligt påkrævet tilfælde, hvor du som dataansvarlig skal foretage en konsekvensanalyse, såfremt den påtænkte behandlingsaktivitet omfatter en systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk behandling, herunder profilering, og som er grundlag for afgørelser, der har retsvirkning for den fysiske person eller på tilsvarende vis betydeligt påvirker den fysiske person.

Du bør overveje, om du foretager evaluering eller analyse, herunder forudsigelse. Særligt hvis det foretages på baggrund af forhold vedrørende den registreredes arbejdsindsats, økonomiske situation, helbred, personlige præferencer eller interesser, pålidelighed eller adfærd eller geografiske position eller bevægelser.

Eksempel
Det kan være en biotekvirksomhed tilbyder genetiske tests direkte til forbrugerne for at vurdere og forudsige sygdomme eller sundhedsrisici.

Det er også relevant for dig som dataansvarlig at overveje, om du behandler personoplysninger med det formål at træffe afgørelser vedrørende specifikke fysiske personer efter en systematisk og omfattende vurdering af deres personlige forhold f.eks. baseret på profilering[3] på baggrund af disse oplysninger.

Eksempel
Hvis politiet f.eks. opsætter fartkameraer og uden nogen form for menneskelig indblanding på baggrund af informationer fra disse udsteder bøder, er der tale om en automatisk afgørelse omfattet af retshåndhævelsesloven. Dette involverer ikke nødvendigvis profilering. Det vil imidlertid nok indebære profilering, såfremt man over tid overvåger enkeltpersoners kørselsvaner og eventuelt indhenter oplysninger om tidligere færdselslovsovertrædelser og anvender dette som grundlag for f.eks. at målrette kontroller mod udvalgte individer.

Den beslutning eller afgørelse, der træffes på baggrund af behandlingsaktiviteten skal have retsvirkning for den fysiske person eller på tilsvarende vis betydeligt påvirke denne. Behandlingsaktiviteten kan f.eks. føre til udelukkelse eller forskelsbehandling af enkeltpersoner. Behandlingsaktiviteter med ringe eller ingen påvirkning af enkeltpersoner opfylder ikke dette specifikke kriterium.

Eksempel
Et andet eksempel er en privat koncertarrangør, der inden afvikling af en større rockkoncert ønsker at vurdere, om der er personer blandt publikum, der kan formodes at udgøre en særlig trussel for andre gæster. Arrangøren vil derfor foretage en samkøring af navnene på de 35.000 personer, der har købt en billet til koncerten op imod offentligt tilgængelige oplysninger (f.eks. medieomtale, blogs mv.), der kan afdække eller indikere, om de pågældende tidligere har optrådt farligt eller forstyrrende ved offentlige arrangementer. En sådan behandling kan siges at ville indebære en høj risiko for de berørte personer og vil have den retsvirkning, at de pågældende nægtes adgang til en koncert, de ellers lovligt har købt billet til. Der skal derfor gennemføres en konsekvensanalyse – ligesom det i øvrigt skal sikres, at databeskyttelsesforordningen krav om proportionalitet mv. efterleves – inden den påtænkte behandlingsaktivitet iværksættes.

4.2. Behandling af (følsomme) oplysninger i stort omfang

Det følger af forordningen, at der ligeledes vil være tale om et særligt påkrævet tilfælde, hvor du som dataansvarlig bør foretage en konsekvensanalyse, såfremt du i stort omfang behandler oplysninger af særlige kategorier eller personoplysninger vedrørende straffedomme eller lovovertrædelser.

For så vidt angår oplysninger af særlige kategorier refereres til de følsomme personoplysninger, der er oplistet i forordningens artikel 9. Dette drejer sig specifikt om personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Derudover drejer det sig om oplysninger vedrørende straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger, som nævnt i forordningens artikel 10.

---

[3] Profilering er i artikel 4, stk. 4, defineret som enhver form for automatisk behandling af personoplysninger, der består i at anvende personoplysningerne til at evaluere bestemte personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den fysiske persons arbejdsindsats, økonomiske situation, helbred, personlige præferencer, interesser, pålidelighed, adfærd, geografisk position eller bevægelser.

Der kan f.eks. være tale om et sygehus, der fører journal over sine patienter.

Er der tale om behandlingsaktiviteter i forbindelse ovenstående kategorier af oplysninger, vil det være særligt påkrævet for dig som dataansvarlig, at foretage en konsekvensanalyse, såfremt behandlingen foretages *i stort omfang*.

Behandling af personoplysninger anses ikke for at ske i "stort omfang"/være "omfattende", blot fordi der er tale om følsomme oplysninger. Der skal være tale om behandling af følsomme oplysninger, *og* der skal ske behandling i stort omfang.

Når du skal vurdere, hvorvidt du behandler oplysninger "i stort omfang", kan du med fordel lægge vægt på de samme kriterier, som der angives i vejledningen om databeskyttelsesrådgivere under afsnittet om, hvorvidt en privat virksomhed er forpligtet til at udpege en databeskyttelsesrådgiver[4]. Det er således relevant at se på

1. Antallet af personer, der behandles oplysninger om – enten det specifikke antal personer eller som andel af befolkningen,

2. Volumen/mængden af personoplysninger og eller volumen/mængden af de forskellige typer af personoplysninger, der bliver behandlet,

3. Tidsperioden, der behandles oplysninger i, samt hvorvidt behandlingen er permanent,

4. Den geografiske udstrækning af behandlingsaktiviteterne.

Behandling af personoplysninger "i stort omfang" kan således indebære behandling af:

- **en stor mængde af personoplysninger**
- **oplysninger om et stort antal personer**
- **lang varighed, herunder permanent**
- **stor geografisk udstrækning af behandlingsaktiviteter**

Eksempel
Som eksempel på behandling af følsomme personoplysninger i stort omfang kan nævnes sundhedsplatformen, som er en platform, der samler informationer om patienter i Region Hovedstaden og Region Sjælland i én samlet elektronisk patientjournal for hver enkelt patient.

[4] Se vejledning om databeskyttelsesrådgivere, afsnit 3.1.2: https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_DPO_-_revideret_offentliggoerelse__1_0_.pdf

Eksempel
Der kan være tale om behandling af personoplysninger i "stort omfang", såfremt der er tale om omfattende behandlingsaktiviteter til behandling af meget store mængder personoplysninger på regionalt, nationalt eller overnationalt plan, der kan berøre mange fysiske personer/registrerede.

"Regionalt" dækker her over behandlingsaktiviteter i dele af Danmark, "nationalt" over behandlingsaktiviteter i hele Danmark mens "overnationalt" dækker over internationale behandlingsaktiviteter, herunder europæiske.

Regionale behandlingsaktiviteter kan være behandlingsaktiviteter inden for sundhedsvæsenet, mens nationale behandlingsaktiviteter f.eks. kan være behandlingsaktiviteter der foretages i landsdækkende forsikringsselskaber.

4.3. Systematisk overvågning af et offentligt tilgængeligt område

Der vil endvidere være tale om et særligt påkrævet tilfælde, såfremt du foretager systematisk overvågning af offentligt tilgængeligt område i stort omfang. Se umiddelbart ovenfor vedrørende vurderingen af "stort omfang".

En konsekvensanalyse er altså ligeledes påkrævet ved omfattende overvågning af offentligt tilgængelige områder, navnlig ved brug af optoelektronisk udstyr. Dette er et særligt påkrævet tilfælde, da personoplysninger kan indsamles under omstændigheder, hvor de registrerede ikke er klar over, hvem der indsamler deres data/oplysninger, og om, hvordan de indsamlede oplysninger vil blive anvendt. Derudover kan det være umuligt for den enkelte at undgå at blive genstand for en sådan behandling i et offentligt tilgængeligt område.

Eksempel
Som eksempel på systematisk overvågning af et offentligt tilgængeligt område kan nævens en kommune eller privat virksomheds opsætning af et antal tv-overvågningskameraer der – inden for rammerne af lov om tv-overvågning – indebærer en løbende overvågning af publikumsområder og lignende.

Tilsvarende er det i det hele taget relevant, hvis du udfører behandlingsaktiviteter, der anvendes til at observere, overvåge eller kontrollere registrerede.

4.4. Tilsynsmyndighedens lister over behandlingsaktiviteter

Den relevante tilsynsmyndighed, hvilket i Danmark vil sige Datatilsynet, udarbejder og offentliggør en liste over de typer af behandlingsaktiviteter, der er underlagt kravet om konsekvensanalyse. Tilsynsmyndigheden kan desuden vælge også at udarbejde en liste over de typer af behandlingsaktiviteter, for hvilke der ikke kræves nogen konsekvensanalyse. Datatilsynet indgiver de udarbejdede lister til Databeskyttelsesrådet. For så vidt angår de lister over behandlingsaktiviteter, hvor der kræves en konsekvensanalyse, afgiver Databeskyttelsesrådet en udtalelse.

Disse lister kan være behjælpelige i din vurdering af, om du skal foretage en konsekvensanalyse. Forordningen angiver ikke en tidfrist for, hvornår disse lister skal foreligge. Det fritager dig ikke for dit ansvar for at foretage en konsekvensanalyse, at listerne ikke foreligger i endelig form. Indtil da må du vurdere behovet for konsekvensanalyse ud fra kriterierne i forordningen, som skitseret i denne vejledning.

Det bemærkes i øvrigt, at du som dataansvarlig har en pligt til at foretage en forudgående høring af Datatilsynet, såfremt en konsekvensanalyse viser, at en behandling, selv efter eventuelt indførte foranstaltninger, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder, jf. afsnit 7 nedenfor.

5. Fælles konsekvensanalyse?

5.1. Flere lignende behandlingsaktiviteter og lignende høje risici

Der kan være tilfælde, hvor det kan være fornuftigt at foretage en konsekvensanalyse, som omfatter mere end ét enkelt projekt.

Dette kan f.eks. være tilfældet, hvis offentlige myndigheder eller organer har planer om at indføre et fælles IT-system eller platform til behandling af personoplysninger.

I stedet for at foretage en konsekvensanalyse for hver påtænkt behandlingsaktivitets konsekvenser for beskyttelse af personoplysninger, er det således muligt at foretage en fælles konsekvensanalyse for flere behandlingsaktiviteter, såfremt der er tale om *lignende behandlingsaktiviteter*, der indebærer *lignende høje risici*.

Det kan være tilstrækkeligt at udarbejde en konsekvensanalyse for flere lignende behandlingsaktiviteter, uanset størrelsen af den mængde data, som behandlingsaktiviteterne omfatter.

5.2. Flere dataansvarlige

Det kan f.eks. være relevant at foretage en fælles konsekvensanalyse, hvis I er flere dataansvarlige, som sammen planlægger at indføre en fælles applikation/IT-system eller behandlingsplatform på tværs af en industrisektor eller industrisegment eller f.eks. inden for den kommunale sektor.

For at I som dataansvarlige kan gå sammen om at lave en fælles konsekvensanalyse, er det en forudsætning, at der er tale om *samme type system*, den *samme behandlingsaktivitet* af de *samme personoplysninger*, samt at behandlingsaktiviteterne *indebærer lignende høje risici*.

Det vil eksempelvis være tilstrækkeligt for flere kommuner at udarbejde én konsekvensanalyse vedrørende databeskyttelse i det samme system – som leveres af samme leverandør – hvis systemet behandler de samme typer af personoplysninger og behandlingsaktiviteterne indebærer samme høje risici.

Eksempel
Flere kommuner ønsker at indkøbe et nyt fagsystem inden for et bestemt kommunalt område, som alle kommuner skal anvende til samme behandlingsaktiviteter. KOMBIT kravsspecificerer systemet på vegne af kommunerne. Viser der sig, at den type behandling, som systemet foretager, kræver udarbejdelse af en konsekvensanalyse, kan KOMBIT i dialog med kommunerne hjælpe med udarbejdelsen af denne fælles konsekvensanalyse. Kommunerne har dog som dataansvarlige fortsat hver især ansvaret for, at konsekvensanalysen udarbejdes.

Det er de dataansvarlige, der konkret vurderer, hvorvidt systemerne og behandlingsaktiviteterne er identiske, herunder gennem en vurdering af indkøbstidspunkt, varierende systemversioner, leverandører mv. Det er som nævnt endvidere væsentligt, at behandlingerne indebærer samme lignende høje risici. Her kan det f.eks. tænkes, at den ene kommune har et tilkøbsmodul til systemet eller en egenudvikling, som vil kræve en konsekvensanalyse, hvis behandlingsaktiviteter heri indebærer høje risici.

I de tilfælde hvor du som dataansvarlig foretager en fælles konsekvensanalyse med flere øvrige dataansvarlige, har I hver især ansvaret for foretagelsen heraf.

Det afgørende er ikke, at der er fuld identitet mellem systemerne og behandlingsaktiviteterne, men at systemet, data og behandlingsaktiviteter ikke afviger væsentligt fra hinanden.

6. Konsekvensanalysens indhold?

Hvis du som dataansvarlig i medfør af de forudgående afsnit har fundet ud af, at du skal lave en konsekvensanalyse, vil de fortegnelser over behandlingsaktiviteter, som du ifølge forordningen skal føre[5], være et godt sted at tage udgangspunkt i, da disse i et vist omfang vil kunne genanvendes ved udarbejdelse af konsekvensanalysen.

Der stilles f.eks. krav om angivelse af formålene med behandlingen ved både udarbejdelse af fortegnelser og konsekvensanalyse. Derudover vil en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger i fortegnelser kunne hjælpe dig i udarbejdelsen af den del af konsekvensanalysen, der vedrører sikkerhedsforanstaltninger, jf. næste afsnit under punkt d.

Som et eksempel på hvordan du kan udføre en konsekvensanalyse vedrørende databeskyttelse, kan nævnes ISO/IEC DIS 29134 "*Information technology – Security techniques – Privacy impact assesment – Guidelines*", som er en international standard udarbejdet af den internationale standardiseringsorganisation, International Organization for Standardization, ISO. Standarden er en vejledning i, hvorledes en konsekvensanalyse (Privacy Impact Assesment proces) kan udføres. Standarden beskriver processen i en række trin, hvoraf et trin f.eks. vedrører identifikation af risici mens et senere trin f.eks. vedrører beslutning om foranstaltninger. Standarden sætter bl.a. fokus på, at behandlingssikkerhed bliver iagttaget og indarbejdet i f.eks. design og implementeringen af IT-løsninger.

Benytter du denne standard ISO/IEC DIS 29134, kan du øge sandsynligheden for at afdække væsentlige elementer i din databehandling og samtidig få vejledning i processen og rapporteringen. Standarden kan både anvendes af offentlige myndigheder og private virksomheder.

6.1. Minimumskrav

En konsekvensanalyse skal *som minimum* indeholde følgende 4 punkter:

a) En systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen, herunder i givet fald de legitime interesser, der forfølges af den dataansvarlige
Dette krav indebærer, at du som dataansvarlig skal foretage en systematisk beskrivelse af de forskellige former for behandling, f.eks. indsamling, registrering, videregivelse mv., som personoplysningerne vil blive genstand for. Du skal endvidere lave en klar beskrivelse og definition af selve de personoplysninger, som skal behandles. Dette gælder også de følsomme personoplysninger om f.eks. race, politiske tilhørsforhold, genetiske data mv.[6], samt personoplysninger vedrørende straffedomme og lovovertrædelser[7].

[5] Se nærmere vejledning om fortegnelse der forventes offentliggjort i januar 2018

[6] Jf. artikel 9, stk. 1, i databeskyttelsesforordningen.

[7] Jf. artikel 10 i databeskyttelsesforordningen.

Konsekvensanalysen skal endvidere indeholde en beskrivelse af formålet med behandlingen, herunder en redegørelse for de legitime interesser du som dataansvarlig har i at behandle oplysningerne. Det kan f.eks. være, at behandlingen af personoplysninger har hjemmel i lov, eller skal ske som led i offentlig myndighedsudøvelse.

b) En vurdering af, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene
Dette krav indebærer, at du som dataansvarlig foretager en vurdering af nødvendigheden af de planlagte behandlinger, og om de er rimelige set i forhold til formålet med behandlingen. Dette krav skal bl.a. være med til at forhindre dataophobning samt til at sikre, at der kun behandles personoplysninger, der er nødvendige, og som kan rummes inden for formålene med behandlingen.

Behandlingen af personoplysninger må altså ikke gå videre, end det der kræves for at opfylde de formål, du som dataansvarlig er berettiget til at forfølge.[8]

c) En vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder
Dette krav indebærer, at du som dataansvarlig foretager en vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder, navnlig retten til beskyttelse af personoplysninger. Det betyder, at du skal vurdere rettighederne i forhold til den planlagte behandling og formålet med behandlingen.

d) De foranstaltninger, der påtænkes for at imødegå disse risici, herunder garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af databeskyttelsesforordningen, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser
Dette krav bør du se i sammenhæng med det forudgående krav. Du skal således vurdere, hvilke foranstaltninger som du påtænker skal imødegå de vurderede risici. Det kan f.eks. være garantier eller sikkerhedsforanstaltninger.

Forskellige påviste risici i en konsekvensanalyse vil således givetvis kræve forskellige foranstaltninger. Se til inspiration f.eks. ISOIIEC 29151 (2017), som er en standard til valg af foranstaltninger til håndtering af påviste risici.

Eksempel
Hvis en risiko f.eks. udspringer af antallet af personer, der har adgang til en stor mængde (følsomme) oplysninger, kan du som sikkerhedsforanstaltning begrænse antallet af sagsbehandlere, der har adgang til at behandle oplysningerne, herunder f.eks. opdele adgang efter hvad den enkelte mere specifikt har behov for, og/eller begrænse den enkeltes muligheder for behandling (læse, ændre, udtrække, samkøre, slette m.v.). Du kan også foretage logning af behandling af personoplysninger (for at finde ud af, hvem der gør hvad, og om der er uvedkommende på netværket) kombineret med kontrol af, om behandlingen er lovlig. Du kan endvidere benytte pseudonymisering, hvis nogle/alle personer kan udføre deres arbejde udelukkende med adgang til pseudonymiserede personoplysninger.

Eksempel
Hvis risiciene blandt andet skyldes, at der sker transmission af oplysninger over internettet eller et andet netværk du ikke har fuld kontrol over, kan en relevant sikkerhedsforanstaltning f.eks. være kryptering af de transmitterede

[8] Se nærmere forordningens artikel 5, stk. 1, litra c og e, vedrørende dataminimering og forbud mod dataophobning.

oplysninger. Krypteringen kan variere i styrke alt efter oplysningernes karakter (hvor følsomme personoplysninger, der er tale om). Sikkerhed for autenticitet og integritet (afsenders og modtager identitet og de transmitterede oplysningers ægthed) kan f.eks. sikres ved elektronisk signatur.

6.2. Konsekvensanalysens udarbejdelse

Databeskyttelsesforordningen præciserer ikke, hvilken procedure for konsekvensanalysen man skal følge. Under forudsætning af, at du tager hensyn til de minimumskrav, der er nævnt umiddelbart ovenfor, kan du indføre en ramme til gennemførelse af konsekvensanalysen på en måde, der supplerer din eksisterende arbejdspraksis.

I artikel 29-gruppens vejledning om konsekvensanalyse[9] er der i bilag 1 henvist til en række tidligere offentliggjorte rammer, som er udviklet af EU's databeskyttelsesmyndigheder, og sektorspecifikke rammer i EU.

6.3. Generel konsekvensanalyse (art. 35, stk. 10)

Det følger af forordningen, at den dataansvarlige i to tilfælde er undtaget fra pligten til at foretage en konsekvensanalyse. Det drejer sig om de tilfælde, hvor behandlingshjemlen skal findes i forordningens artikel 6, stk. 1, litra c og e.

Du skal altså se, om der er tale om en behandling, der er nødvendig for at overholde en retlig forpligtelse, der påhviler dig som dataansvarlig, eller er der tale om en behandling, der er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som du som dataansvarlig har fået pålagt.

Er dette tilfældet, *og* har behandlingen i øvrigt et retsgrundlag i EU-retten eller i national ret, som du er underlagt, *og* regulerer denne ret den eller de pågældende specifikke behandlingsaktiviteter, *og* er der allerede foretaget en generel konsekvensanalyse i forbindelse med vedtagelsen af dette retsgrundlag, så er du undtaget fra en eventuel pligt efter forordningen til at skulle foretage en konsekvensanalyse.

I Danmark vil det i praksis betyde, at en generel konsekvensanalyse vil kunne foretages i forbindelse med udformningen af et lovforslag eller eventuelt en bekendtgørelse.

6.4. Fornyet konsekvensanalyse

Såfremt risikobilledet ændrer sig, eller du af anden grund vurderer, at det er nødvendigt, skal du som dataansvarlig foretage en fornyet gennemgang af behandlingsaktiviteterne med henblik på at vurdere, hvorvidt behandlingen er foretaget i overensstemmelse med den oprindelige konsekvensanalyse. Dette skal f.eks. ske, når der sker en sådan ændring, at den risiko, som behandlingsaktiviteterne udgør, bliver højere.

Når der sker ændringer, som betyder, at formålet med behandlingen ændres, skal du ligeledes vurdere, om der er behov for en fornyet gennemgang.

---

[9] Tilgængelig på Datatilsynets hjemmeside: www.datatilsynet.dk

Ændres behandlingen, således at der fremover skal behandles andre personoplysninger, end dem der aktuelt behandles, skal du også vurdere, om der er behov for en fornyet gennemgang.

Det kan f.eks. tænkes, at et system fremover skal behandles følsomme personoplysninger såsom fagforeningsmæssige tilhørsforhold eller politisk overbevisning og ikke kun oplysninger om f.eks. navn og adresse. Det kan eksempelvis også være, at et system, der omfatter behandlingsaktiviteter af følsomme personoplysninger[10] fremover også skal omfatte behandling af oplysninger om straffedomme[11].

[10] Omfattet af forordningens artikel 9

[11] Omfattet af forordningens artikel 10

7. Forudgående høring af tilsynsmyndigheden

Visse behandlinger kræver, at tilsynsmyndigheden, høres forud for påbegyndelse af behandlingen.

Det er dog vigtigt at være opmærksom på, at det er dit ansvar som dataansvarlig at vurdere, om en behandling – herunder indsamling, registrering og videregivelse – er i overensstemmelse med forordningen. En udtalelse fra Datatilsynet på baggrund af din høring vil ikke gøre op med eller godkende alle fremtidige databehandlinger, der vil ske hos dig som led i de behandlingsaktiviteter, du har hørt tilsynet om.

7.1. Hvornår skal der foretages forudgående høring af tilsynsmyndigheden?

Du har pligt til at foretage en forudgående høring af Datatilsynet, inden du påbegynder en påtænkt behandling af personoplysninger, hvis din konsekvensanalyse viser, at behandlingen *vil* føre til en høj risiko, og du ikke kan begrænse denne høje risiko ved indførelse af passende foranstaltninger.

Er du en privat dataansvarlig, skal du endvidere i visse situationer altid indhente forudgående tilladelse fra Datatilsynet, inden du påbegynder behandlingen.

Ved udarbejdelse af lovforslag, bekendtgørelser, cirkulærer eller lignende generelle retsforskrifter, som omhandler behandling af personoplysninger, skal der indhentes en udtalelse fra Datatilsynet med henblik på at sikre, at den planlagte behandling overholder forordningen, og navnlig for at begrænse risiciene for den registrerede.

7.2. Tilsynsmyndighedens reaktion

Datatilsynet skal reagere, såfremt tilsynet finder, at den planlagte behandling overtræder forordningen. Overtrædelse kan navnlig foreligge, hvis du ikke i tilstrækkelig grad har identificeret eller begrænset den foreliggende risiko. Men overtrædelse kan f.eks. også foreligge, hvis de påtænkte behandlingsaktiviteter går videre, end hvad der er muligt efter forordningens betingelser.

Når Datatilsynet har identificeret en overtrædelse, skal tilsynet give dig eller din databehandler skriftlig rådgivning. Dette skal ske inden for en periode på op til otte uger efter modtagelse høringsanmodningen. Datatilsynet kan i den forbindelse anvende enhver af de beføjelser, tilsynet er tillagt efter forordningen, f.eks. adgangen til at kræve yderligere oplysninger[12].

Datatilsynets manglende reaktion inden for det fastsatte tidsrum (der i visse situationer kan forlænges eller suspenderes) berører ikke dets mulighed for at gribe ind i overensstemmelse med dets tillagte beføjelser og opgaver, herunder f.eks. beføjelsen til at forbyde behandlingsaktiviteter.

[12] For en nærmere oplistning af beføjelserne henvises til forordningens artikel 58.

Hvis Datatilsynet *ikke* finder, at den planlagte behandling overtræder forordningen, er der ikke et krav om skriftlig vejledning. Det er i den forbindelse også vigtigt at være opmærksom på, at du *ikke* kan antage, at en manglende reaktion fra Datatilsynet er udtryk for, at enhver kommende/fremtidig databehandling i forbindelse med den aktivitet, der er forelagt Datatilsynet, er i overensstemmelse med forordningen. Datatilsynet kan således fortsat gribe ind i overensstemmelse med sine beføjelser.

7.3. Grundlaget for tilsynsmyndighedens behandling

I forbindelse med høringen af Datatilsynet skal du indgive de oplysninger til tilsynet, som fremgår af nedenstående boks.

Som dataansvarlig skal du oplyse Datatilsynet om følgende i forbindelse med en påkrævet høring (art. 36, stk. 3):

- **ansvarsområderne for henholdsvis den dataansvarlige, fælles dataansvarlige og databehandleren, der er involveret i behandlingen, navnlig med hensyn til behandlingen inden for en koncern,**
- **den planlagte behandlings formål og hjælpemidler,**
- **foranstaltninger og garantier til beskyttelse af de registreredes rettigheder og frihedsrettigheder,**
- **databeskyttelsesrådgiverens kontaktoplysninger,**
- **konsekvensanalysen,**
- **andre oplysninger som tilsynsmyndigheden anmoder om.**

I relation til første punkt menes f.eks. en angivelse af rollerne og ansvarsområderne for de nævnte aktører (f.eks. hvilken rolle og ansvarsområde databehandleren har). For så vidt angår "hjælpemidler" i andet punkt menes bl.a., hvilke midler der anvendes til at foretage behandlingen (hvordan foretages behandlingen).

Som det også fremgår af boksens sidste punkt, har du pligt til at give andre oplysninger, som Datatilsynet anmoder om, hvilket f.eks. kan være oplysninger om, hvor personoplysningerne vil blive behandlet, herunder om du f.eks. har en databehandler uden for EU, og på hvilket grundlag overførsler af oplysninger til tredjelandet vil ske.

8. Indhentelse af den registreredes synspunkter

For at sikre den bedste databeskyttelse, bør du som dataansvarlig være omhyggelig ved udførelsen af en konsekvensanalyse.

Hvis det er relevant, bør du indhente de registreredes eller deres repræsentanters synspunkter vedrørende den planlagte behandling. Det skal gøres uden, at det berører beskyttelse af kommercielle eller samfundsmæssige interesser eller behandlingsaktiviteternes sikkerhed.

Hvorvidt det er relevant afhænger af en konkret vurdering af risiciene for de registrerede, hver gang du foretager en behandling.

Det kan eksempelvis være relevant at indhente synspunkter fra den registrerede eller dennes repræsentant i forbindelse med høringsprocessen ved udarbejdelse af lovforslag.

Artikel 29-gruppen har i sin vejledning om konsekvensanalyser angivet, at disse synspunkter kan indhentes ved hjælp af forskellige midler afhængigt af situationen – f.eks. en generel undersøgelse i relation til formålet med og hjælpemidlerne til behandlingsaktiviteten, et spørgsmål til medarbejderrepræsentanterne eller almindelige undersøgelser, der sendes til den dataansvarliges fremtidige kunder – der sikrer, at den dataansvarlige har et retsgrundlag for behandling af personoplysninger i forbindelse med indhentningen af sådanne synspunkter.

9. Adfærdskodekser

En adfærdskodeks er i databeskyttelsesforordningens forstand et sæt retningslinjer, som skal bidrage til at sikre, at de virksomheder, der har tilsluttet sig kodeksen, anvender reglerne i databeskyttelsesforordningen korrekt. En adfærdskodeks kan f.eks. gå ud på at specificere databeskyttelsesforordningens regler om behandlingssikkerhed.

Overholdelse af en godkendt adfærdskodeks kan således bruges som element til at påvise, at du som dataansvarlig lever op til dine forpligtelser efter forordningen.

Derfor følger det også direkte af forordningen, at overholdelse af godkendte adfærdskodekser skal inddrages behørigt ved vurderingen af konsekvenserne af de behandlingsaktiviteter, der udføres den dataansvarlige eller databehandlere, navnlig i forbindelse med en konsekvensanalyse.

Eksempel[13]
Er du f.eks. et (privat)hospital[14], der ønsker at indkøbe et nyt IT-system, hvor du bl.a. vil registrere og behandle oplysninger om alle dine patienter, så skal du (formentlig) foretage en konsekvensanalyse inden IT-systemet tages i brug, idet der behandles følsomme personoplysninger (helbredsoplysninger) i stort omfang.

I den forbindelse kan det være, at du tidligere har tilsluttet dig en godkendt adfærdskodeks vedrørende behandlingssikkerhed (for så vidt angår personoplysninger) på (privat)hospitaler. Adfærdskodeksen indeholder bl.a. klare retningslinjer for pseudonymisering og kryptering af personoplysninger samt klare retningslinjer for privathospitalers beskyttelse af personoplysninger ud mod internettet (firewalls mv.). Når du skal foretage din konsekvensanalyse, vil du kunne inddrage efterlevelsen af den godkendte adfærdskodeks vedrørende behandlingssikkerhed, når du skal vurdere risikoen ved at overgå til det nye it-system. Adfærdskodeksen kan på denne måde bidrage til at mindske risikoen ved at tage det nye it-system i brug.

[13] Se nærmere om adfærdskodekser i vejledning om adfærdskodekser og certificeringsordninger, hvor eksemplet ligeledes fremgår fsva. et privathospital, der er tilgængelig på Datatilsynets hjemmeside: www.Datatilsynet.dk

[14] Eller et landsdækkende forsikringsselskab, der tegner syge- og ulykkesforsikringer

10. Opsummering

Denne vejledning skulle gerne have givet dig som dataansvarlig nærmere information om, hvornår du skal foretage en konsekvensanalyse, og hvad den skal indeholde.

Nedenstående er en opsummering af vejledningens opmærksomhedspunkter

- Du er, som dataansvarlig, forpligtet til at foretage en konsekvensanalyse, når en behandling *sandsynligvis* vil indebære en *høj risiko* for fysiske personers rettigheder og frihedsrettigheder, navnlig ved brug af "nye teknologier", herunder anvendelse af teknologier på nye måder.

- En konsekvensanalyse er navnlig påkrævet, hvis 1) der sker en systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk behandling, herunder profilering, 2) der behandles følsomme oplysninger i stort omfang, eller 3) der sker systematisk overvågning af et offentligt tilgængeligt område i stort omfang.

- En konsekvensanalyse kan omfatte flere lignende behandlingsaktiviteter, der indebærer lignende høje risici.

- En konsekvensanalyse skal *mindst* omfatte 1) en systematisk beskrivelse af behandlingsaktiviteterne og formålene med behandlingen 2) en proportionalitetsvurdering i forhold til formålene 3) en vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder 4) de foranstaltninger der påtænkes for at imødegå disse risici.

- Såfremt risikoen ved behandlingsaktiviteten ændrer sig, skal du som dataansvarlig foretage en fornyet gennemgang. Det kan også være nødvendigt af andre grunde.

- Hvis konsekvensanalysen viser, at behandlingen *vil* føre til en høj risiko, og du *ikke* begrænser denne høje risiko ved indførelse af passende foranstaltninger, har du pligt til at høre Datatilsynet inden påbegyndelse af behandlingen.

- Overholdelse af godkendte adfærdskodekser skal inddrages behørigt ved vurderingen af konsekvenserne i forbindelse med en konsekvensanalyse.

Dato
22. marts 2018

Justitsministeriet
Slotsholmsgade 10
1216 København K

Telefon
72 26 84 00

Email
jm@jm.dk

ISBN
978-88-98564-35-7

Foto
Scanp