Dansk persondataret

Bent Ole Gram Mortensen (red.)

Dansk persondataret

Ex Tuto
PUBLISHING
www.extuto.com

Bent Ole Gram Mortensen (red.), Carina Risvig Hamer, Daniel Hartfield-Traun, Lisa Hjerrild, Kent Kristensen, Jesper Kruse Markvart, Helene Arensbak Mørk, Jesper Løffler Nielsen, Ayo Næsborg-Andersen, Sten Schaumburg-Müller, Christian Højer Schjøler, Peter Starup, Jøren Ullits & Frederik Waage
Dansk persondataret
Første udgave, første oplag

Denne bog er udgivet i januar 2020 af Ex Tuto Publishing A/S. Grafisk tilrettelæggelse og sats af mere.info A/S, som har anvendt LibreOffice/Linux samt skrifterne Baskerville Original og Cronos designet af henholdsvis František Štorm i 2000 og Robert Slimbach i 1996. Jan Trzaskowski har stået for forlagsredaktion og Tove Møgelvang-Hansen har været ansvarlig for korrekturlæsning. Bogen er trykt på Munken Pure 100 g/m^2 af Narayana Press, der ligger på Gyllingnæs syd for Odder. Indbindingen er udført af Buchbinderei S.R. Büge GmbH i Celle. Bogen er fagfællebedømt.

Ex Tuto A/S er medlem af Forening for Boghaandværk, og vi støtter bæredygtig skovforvaltning ved at anvende FSC-certificeret papir.

Printed in Denmark 2020
ISBN 978-87-420-0033-5

Ex Tuto Publishing A/S
Toldbodgade 55, 1.
DK-1253 København K
www.extuto.com

MIX
Papir fra ansvarlige kilder
FSC® C010651
www.fsc.org

Udgivet med støtte fra
dreyersfond

FairPublishing

Kapiteloversigt

Kapitel 12

Krav om konsekvensanalyse

Lisa Hjerrild

12.1. Indledning

Med databeskyttelsesforordningen (GDPR) er dataansvarlige pålagt en række forpligtelser ved behandling af persondata, sådan som det også er behandlet i de foregående kapitler. Såfremt en behandling af persondata vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, er den dataansvarlige forpligtet til at foretage en *analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger*, som kort blot kaldes for en "konsekvensanalyse". På engelsk hedder konsekvensanalysen *Data Protection Impact Assessment* (DPIA). Undertiden anvendes forkortelsen DPIA også i dansk dataretlig terminologi. I det følgende vil den blive omtalt som en *konsekvensanalyse*.

Konsekvensanalysen skal laves af den dataansvarlige forud for den påtænkte behandling og skal i nogle tilfælde sendes til forudgående høring hos Datatilsynet. Konsekvensanalysen skal ses som en essentiel del af overholdelsen af forordningen, når der planlægges eller foretages databehandling med høj risiko for de registrerede. Formålet med analysen, hvem der skal udarbejde en, og hvad konsekvensanalysen skal indeholde, vil blive gennemgået nedenfor.

Regelgrundlaget for konsekvensanalyser findes i forordningens artikel 35 og 36, som indeholder de formelle og materielle bestemmel-

ser om den dataansvarliges forpligtelse til i visse situationer at udarbejde en konsekvensanalyse. Bestemmelserne om konsekvensanalyser er suppleret af retningslinjer og vejledninger som hjælp til at forstå reglerne. Artikel 29-Gruppen for Databeskyttelse (Nu Det Europæiske Databeskyttelsesråd eller blot Databeskyttelsesrådet) har udarbejdet *Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679 (WP 248)*.[1] Retningslinjerne er tiltrådt af Det Europæiske Databeskyttelsesråd. Datatilsynet har udgivet *Vejledning om Konsekvensanalyse*.[2] Formålet med vejledningen er at hjælpe dataansvarlige med at håndtere konsekvensanalyser.[3]

12.2. Formålet med en konsekvensanalyse

Konsekvensanalysen kan ses som det forlængede led af den almindelige risikovurdering.[4] I de tilfælde, hvor den dataansvarlige vurderer, at der er *høj* risiko for at krænke de registreredes rettigheder, skal der foretages en konsekvensanalyse.[5] Konsekvensanalysens formål består af to dele: det skal dels hjælpe med at vurdere mulige risici for registreredes rettigheder og frihedsrettigheder, dels fastlægge foranstaltninger for at imødegå disse risici.

Konsekvensanalysen hjælper dermed til at identificere og begrænse de konkrete risici ved en given behandling. Konsekvensanalysens resultat kan og bør dermed inddrages, når der skal træffes passende foranstaltninger med henblik på at påvise, at behandlingen af personoplysninger overholder de databeskyttelsesretlige regler.

Det er den dataansvarliges ansvar, at der udarbejdes en konsekvensanalyse i overensstemmelse med artikel 35, men er det reelt en databehandler, der foretager databehandlingen, skal denne assistere den dataansvarlige med at udføre konsekvensanalysen.[6] Har organisationen en databeskyttelsesrådgiver (DPO), vil denne også skulle assi-

1. Artikel 29-Gruppen WP 248 rev.01.
2. Datatilsynet 2018a.
3. Ibid., s. 2.
4. Se mere herom i kapitel 14.
5. Se GDPR artikel 35.
6. GDPR præambelbetragtning nr. 95.

stere og rådgive i forbindelse med udarbejdelsen af konsekvensanalyser og en eventuel høring af Datatilsynet.[7]

12.3. Hvornår er konsekvensanalysen påkrævet? (artikel 35)

Hvornår dataansvarlige skal foretage en konsekvensanalyse, er fastlagt i databeskyttelsesforordningens artikel 35, stk. 1:

> "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. En enkelt analyse kan omfatte flere lignende behandlingsaktiviteter, der indebærer lignende høje risici."

Det betyder, at der kun skal udarbejdes en konsekvensanalyse i de tilfælde, hvor der sandsynligvis vil være en høj risiko for krænkelse af fysiske personers rettigheder og frihedsrettigheder. Konsekvensanalysen udarbejdes typisk i forlængelse af risikovurderingen.[8] Der skal altid udarbejdes en risikovurdering, men det er kun i de tilfælde, hvor der sandsynligvis er en høj risiko for de registrerede, der også skal udarbejdes en konsekvensanalyse.[9]

Den høje risiko for registrerede kan eksempelvis opstå som følge af behandling af personoplysninger, der kan føre til fysisk, materiel eller immateriel skade, hvilket kan være tilfældet, hvis behandlingen giver anledning til identitetstyveri, forskelsbehandling, skade på omdømme, eller hvis de registrerede bliver frarøvet deres rettigheder eller forhindret i at kontrollere de registrerede personoplysninger.[10] Konse-

7. Jf. GDPR artikel 39, stk. 1, litra c. Databeskyttelsesrådgiveren (DPO) skal blandt andet bistå den dataansvarlige med rådgivning om databeskyttelse og overvåge overholdelsen af databeskyttelsesforordningen. DPO'ens opgaver og ansvar er selvstændigt omtalt i kapitel 11.
8. Se også kapitel 14.
9. Se artikel 35.
10. Se præambelbetragtning nr. 83 og 89 og Datatilsynet 2018a, s. 7.

kvensanalysen skal særligt foretages med henblik på at vurdere den høje risikos oprindelse, karakter, særegenhed og alvor. Derfor bør den dataansvarlige også ved vurdering af datasikkerhedsrisikoen[11] tage hensyn til de risici, som behandling af personoplysninger indebærer, såsom hændelig eller ulovlig tilintetgørelse, tab, ændring eller uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet, og som navnlig kan føre til fysisk, materiel eller immateriel skade.

12.3.1. Sædvanlig behandling og nye teknologier

Især ved en planlagt anvendelse af nye teknologier eller en ny anvendelse af eksisterende teknologier skal dataansvarlige være særligt opmærksomme. Ved nye teknologier er det nødvendigt at være ekstra opmærksom på, om der indsamles personoplysninger på en ny måde, som hidtil har været ukendt. Dertil er konsekvensanalysen et vigtigt redskab til at beskytte de registreredes rettigheder og frihedsrettigheder ved at hjælpe til at forstå og behandle mulige risici. Der skal være tale om reelt nye teknologier og ikke eksempelvis udskiftning af et it-system.[12] I vurderingen af, om teknologien er ny, skal der ses på bl.a., hvordan teknologiudviklingen er i det omkringværende samfund. Omvendt anvender forordningen terminologien "navnlig", hvilket må betyde, at det ikke kan udelukkes, at der også ved udskiftning af it-systemer, som er væsentlig forandrede, kan være behov for at udarbejde en konsekvensanalyse.

Eksempler på nye teknologier kan være biometrisk data til identifikation og genkendelse af personer ved hjælp af unikke biologiske kendetegn, f.eks. elektronisk genkendelse af ansigt, øjne, fingre, stemme, blodårer eller gangarter.[13] Eksemplet viser i øvrigt, at der ikke nødvendigvis er tale om ny teknologi ved anvendelse af biometrisk data, men det kan efter omstændighederne blive anset for at være ny teknologi, hvis det anvendes på en ny måde. Andre eksempler er Internet of Things (IoT), elektroniske identiteter og kunstig intelligens.

11. Se også kapitel 14.
12. Datatilsynet 2018a, s. 5 ff.
13. Ibid., s. 6.

12.3.2. De særligt påkrævede tilfælde – artikel 35, stk. 3

En konsekvensanalyse er navnlig påkrævet i følgende tre tilfælde:[14] *For det første* er en konsekvensanalyse navnlig påkrævet ved *persondatabehandling, der indebærer 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.[15] Det kan eksempelvis være tilfældet, hvis en dataansvarlig udarbejder evalueringer, analyser eller træffer afgørelser. Dette gælder især, hvis afgørelserne træffes på baggrund af profilering.[16]

Som *det andet tilfælde* skal en konsekvensanalyse navnlig udarbejdes, hvor der sker *behandling i stort omfang af særlige kategorier af oplysninger*,[17] eller *af personoplysninger vedrørende straffedomme og lovovertrædelser*.[18] Hvis en dataansvarlig behandler følsomme personoplysninger, såsom eksempelvis race, etnisk oprindelse, politisk, filosofisk eller religiøs overbevisning eller genetiske eller helbredsoplysninger i stort omfang, bør det altid overvejes, om der skal udarbejdes en konsekvensanalyse. Det typiske eksempel er et hospital, som er forpligtet til at føre patientjournaler. Når det skal vurderes, om der er tale om et "stort omfang", skal der særligt ses på mængden af personoplysninger, antallet af personer, varigheden og den geografiske udstrækning.[19]

For det tredje skal en konsekvensanalyse navnlig udarbejdes, hvis der sker *systematisk overvågning af et offentligt tilgængeligt område i stort*

14. Forordningens artikel 35, stk. 3.
15. Jf. artikel 35, stk. 3, litra a.
16. Profilering er defineret som enhver form for automatisk behandling af personoplysninger, der består i at anvende personoplysninger 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, jf. GDPR artikel 4, stk. 4.
17. De følsomme personoplysninger, jf. artikel 9, stk. 1.
18. Jf. GDPR artikel 35, stk. 3, litra b.
19. Om vurderingen af hvornår der er tale om et stort omfang, kan der også henvises til afsnit 12.3.2. ovenfor.

omfang.[20] Ved offentlig overvågning kan det være henved umuligt for den enkelte at undgå at blive genstand for en databehandling på baggrund af registreringerne. Baggrunden for at medtage disse situationer, hvor der sker overvågning af et offentligt tilgængeligt område i stort omfang, er navnlig hensynet til den registrerede, som (måske) ikke er klar over, hvem der registrerer deres data/oplysninger, og til hvilke formål de bliver anvendt. For så vidt angår vurderingen af, hvornår der er tale om et "stort omfang", kan der henvises til beskrivelsen umiddelbart ovenfor.

12.3.3. Tilsynsmyndighedens lister over type-behandlinger, hvor en konsekvensanalyse er påkrævet/ikke-påkrævet

Datatilsynet er som Danmarks nationale tilsynsmyndighed forpligtet til at udarbejde og offentliggøre lister over de typer af behandlingsaktiviteter, hvor der altid skal udarbejdes en konsekvensanalyse.[21] Når Datatilsynets udkast til liste er udarbejdet, skal udkastet til listen forelægges Det Europæiske Databeskyttelsesråd til udtalelse om de situationer, hvor det er obligatorisk at udarbejde en konsekvensanalyse. Herefter bliver udkastet behandlet på et møde, hvor Databeskyttelsesrådet tager stilling til, om listen vil medføre en inkonsekvent anvendelse af kravet om konsekvensanalyser på tværs af medlemsstaterne. Forelæggelsen skal understøtte den sammenhængskraft, som forordningen skal repræsentere, og sikre, at der sker en harmonisering på tværs af medlemsstaterne, for hvilke behandlingsaktiviteter der altid kræver udarbejdelse af en konsekvensanalyse. Senest har Datatilsynet den 4. december 2018 fået godkendt den danske liste over behandlingsaktiviteter, hvor der altid skal udarbejdes en konsekvensanalyse. Af listen fremgår bl.a. behandling af persondata, der fører til afgørelser om en fysisk persons rettigheder til et produkt, der er baseret på en hvilken som helst form for automatiseret afgørelse (herunder profilering), behandling, der omfatter profilering af fysiske personer i stor skala, hvor der benyttes profilering eller andre former for automatiserede afgørelser, og behandlinger, hvor et brud på persondatasikkerheden kan have en direkte

20. Jf. GDPR artikel 35, stk. 3, litra c.
21. GDPR artikel 35, stk. 4.

effekt på en persons fysiske helbred eller på sikkerheden for en fysisk person.

Datatilsynet kan endvidere frit vælge også at udarbejde og offentliggøre lister over de typer af behandlingsaktiviteter, hvor tilsynet har vurderet, at der ikke kan stilles krav om konsekvensanalyse.[22] Det kan eksempelvis være situationer, hvor Datatilsynet tidligere har vurderet, at en given overvågning af et offentligt område ikke sker i et stort omfang og derfor ikke kræver, at der skal udarbejdes en konsekvensanalyse. Den frivillige liste skal dog også forelægges Databeskyttelsesrådet, som kan give udtalelse for at sikre harmonisering på tværs af medlemsstaterne. Uanset om en given behandlingsaktivitet fremgår af listen over behandlingsaktiviteter, hvor der ikke umiddelbart skal udarbejdes en konsekvensanalyse, er det altid den dataansvarliges ansvar at vurdere, hvorvidt der alligevel skal udarbejdes en konsekvensanalyse, fordi en konkret behandlingssituation alligevel er omfattet af kravene.

12.3.4. Undtagelse fra kravet om konsekvensanalyse

Dataansvarlige er i to tilfælde undtaget fra pligten til at foretage en konsekvensanalyse.[23]

- Hvor behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige[24] *eller*
- Hvor behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.[25]

Hvis en af de to situationer gør sig gældende, og behandlingen har hjemmel i EU-retten eller i national ret, som den dataansvarlige er underlagt, og er der allerede foretaget en generel konsekvensanalyse i forbindelse med vedtagelsen af dette retsgrundlag, er den dataansvar-

22. GDPR artikel 35, stk. 5.
23. GDPR artikel 35, stk. 10.
24. Situationer hvor den dataansvarliges behandlingshjemmel følger af GDPR artikel 6, stk. 1, litra c.
25. Den dataansvarliges behandlingshjemmel følger af artikel 6, stk. 1, litra e.

lige undtaget fra en eventuel pligt efter forordningen til at skulle foretage en konsekvensanalyse.

I praksis betyder det, at en generel konsekvensanalyse vil kunne foretages i forbindelse med det lovforberedende arbejde ved udformningen af et lovforslag eller eventuelt en bekendtgørelse. Det kan i sådanne tilfælde medføre, at en dataansvarlig er undtaget fra kravet om at udarbejde en konsekvensanalyse.

12.3.5. Fælles konsekvensanalyse

Ved samarbejder på tværs af organisationer med flere involverede dataansvarlige kan der opstå tilfælde, hvor det kan være rimeligt og økonomisk hensigtsmæssigt at udarbejde en konsekvensanalyse, som omfatter mere end ét enkelt projekt, f.eks. hvis offentlige myndigheder eller organer har planer om at indføre en fælles app eller behandlingsplatform eller en app på tværs af sektorer.[26]

12.4. Krav til konsekvensanalysen

Forordningen stiller en række mindstekrav til indholdet af en konsekvensanalyse, som den dataansvarlige altid skal forholde sig til.[27] Derudover kan – og hvis relevant skal – den dataansvarlige inddrage andre relevante elementer, hvor det vurderes at være relevant.

Konsekvensanalysen skal som minimum omfatte:

1. En *systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene* med behandlingen, herunder i givet fald de legitime interesser, der forfølges af den dataansvarlige,
2. en vurdering af, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene (en *proportionalitetsvurdering*),
3. en vurdering af *risiciene for de registreredes rettigheder og frihedsrettigheder*, og
4. angivelse af de *foranstaltninger*, den dataansvarlige påtænker at indføre for at begrænse og imødegå disse risici, herunder garan-

26. GDPR præambelbetragtning nr. 92.
27. GDPR artikel 35, stk. 7.

> tier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af forordningen, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser.

Alle fire punkter skal være fyldestgørende beskrevet i konsekvensanalysen, der gerne må indeholde yderligere beskrivelser for håndtering af behandlingssikkerheden. Der er ikke krav om, at den dataansvarlige skal offentliggøre konsekvensanalysen, men der er modsat heller ikke et forbud imod at gøre det. Datatilsynet anser det dog for en god mulighed for at skabe bedre gennemsigtighed for den registrerede til at vurdere egen risiko.

12.5. Forudgående høring (artikel 36)

12.5.1. Høring af tilsynsmyndigheden

Efter at den dataansvarlige har udarbejdet en konsekvensanalyse og iværksat passende foranstaltninger for at begrænse risikoen (f.eks. ved kryptering og kontrolmekanismer), skal den dataansvarlige efter artikel 36 vurdere, hvorvidt foranstaltningerne i tilstrækkelig grad gør op med den høje risiko. Det er den dataansvarliges ansvar at foretage denne vurdering, og såfremt den dataansvarlige vurderer, at der fortsat er høj risiko, skal den dataansvarlige høre og indhente tilladelse fra Datatilsynet og eventuelt også de registrerede forud for iværksættelse af behandlingen.[28]

Ved høring af Datatilsynet skal den dataansvarlige indsende en række oplysninger til tilsynet.[29] Det er den dataansvarlige, der skal foretage vurderingen af, om Datatilsynet skal høres, eller om de iværksatte foranstaltninger er tilstrækkelige til at imødegå den høje risiko.

Den dataansvarlige skal angive ansvarsfordelingen mellem henholdsvis den dataansvarlige, fælles dataansvarlige og databehandleren, der er involveret i behandlingen, sammen med den konkrete konsekvensanalyse i medfør af artikel 35.[30] En beskrivelse af rollefordelingen

28. GDPR artikel 36.
29. GDPR artikel 36, stk. 3, litra a-f.
30. GDPR artikel 36, stk. 3, litra a.

er især relevant, når den dataansvarlige og databehandleren indgår i koncernforhold. Derudover skal behandlingens formål og hjælpemidler oplyses og beskrives, samt angive foranstaltningerne og garantierne til beskyttelse af de registreredes rettigheder og frihedsrettigheder i henhold til databeskyttelsesforordningen.[31] Kontaktoplysninger på databeskyttelsesrådgiveren kan også medsendes. Endvidere skal den dataansvarlige fremsende eventuelle andre oplysninger, som Datatilsynet anmoder om.

Datatilsynet skal reagere inden for en fastsat frist, hvis det finder, at den påtænkte behandling er i strid med forordningen.[32] Fristen er op til otte uger for Datatilsynet til at reagere.[33] Det kan eksempelvis tænkes, at Datatilsynet finder, at den dataansvarlige ikke i tilstrækkeligt omfang har foretaget foranstaltninger til at begrænse den registreredes risiko eller ikke har identificeret alle relevante risici. Har Datatilsynet ved udløbet af fristen ikke reageret, må den dataansvarlige som udgangspunkt kunne gå ud fra, at man kan iværksætte den påtænkte behandling.

12.5.2. Indhentelse af registreredes synspunkter

Datatilsynet anbefaler, at den dataansvarlige indhenter synspunkter fra de registrerede eller deres repræsentanter forud for en påtænkt behandling også ved den forudgående høring ved konsekvensanalyser.[34] De registreredes repræsentanter kan eksempelvis være forbrugerrepræsentanter eller fagforeninger som repræsentanter for arbejdstagere.

31. GDPR artikel 36, stk. 3, litra b og c.
32. Om Datatilsynets reaktionsmuligheder se også GDPR artikel 58 og Datatilsynet 2018a, s. 21.
33. GDPR artikel 36, stk. 2.
34. Datatilsynet 2018a, s. 23.