Rådet for Digital Sikkerhed

12. februar 2021

Konsekvensanalyse i praksis

Anvendelsen af konsekvensanalyser efter databeskyttelsesforordningen har ikke vundet særlig stor udbredelse. Årsagerne er bl.a. tvivl om, hvornår der skal gennemføres konsekvensanalyser, og tvivl om hvordan de skal gennemføres. Rådet for Digital Sikkerhed har derfor nedsat en tværsektoriel ekspertgruppe til at udarbejde en skabelon for gennemførsel af konsekvensanalyser og til at skitsere en række cases, hvor konsekvensanalyser bør og ikke bør gennemføres, herunder eksempler på konsekvenser for den registrerede der medfører krav om konsekvensanalyse. Vejledningen indeholder en tjekliste til 1) hvornår og 2) hvordan der skal gennemføres konsekvensanalyser. Rådet håber, at det med udgivelsen af denne vejledning, vil blive lettere at gå til arbejdet med at gennemføre konsekvensanalyser.

Om vejledningen

Konsekvensanalyser ved behandling af personlysninger er i en række situationer gjort obligatoriske efter databeskyttelsesforordningens artikel 35. Konsekvensanalyser er imidlertid ikke et meget anvendt redskab, og de første organisationer er kun så småt i gang med at gøre sig erfaringer med anvendelse af konsekvensanalyser. Datatilsynet har i skrivende stund ikke modtaget nogle henvendelser efter artikel 36, hvor der er stor risiko for de registrerede, og det kan konstateres, at der i praksis er væsentlige udfordringer med at efterleve formkravene i artikel 35. Rådet for Digital Sikkerhed har derfor taget initiativ til - sammen med en række eksperter på området - at udarbejde en vejledning om konsekvensanalyser. På den måde kan man tage sine passende forholdsregler og evt. gennemføre sin ønskede databehandling.

Med databeskyttelsesforordningens artikel 35 fastslås, at *der skal gennemføres en konsekvensanalyse*, når behandlingen af personoplysninger udgør en høj risiko for de registreredes rettigheder.

Denne vejledning har til formål at udbrede kendskabet til konsekvensanalyser, at bidrage til en vurdering af hvornår der skal gennemføres konsekvensanalyser, og at skitsere en metodik for hvordan man kan gennemføre konsekvensanalyser i praksis. Målgruppen er især mindre offentlige eller private organisationer, der kan have behov for at gennemføre mindre konsekvensanalyser, og som ikke har et stort setup til at gennemføre analyserne. Vejledningen er meget fokuseret på at opnå praktiske resultater.

Vejledningen er blevet udarbejdet med bidrag fra:
- Henning Mortensen, Rådet for Digital Sikkerhed (redaktør)
- Allan Frank, Datatilsynet
- Helle Uldbæk Sørensen, Statens IT
- Anders Chemnitz, Nyborg Kommune
- Sille Larsen Nielsen, Frederiksberg Kommune
- Alexander Trolle, Nets.

Indhold

1. Fra risikovurdering til konsekvensanalyse

Det er med databeskyttelsesforordningen blevet obligatorisk for den dataansvarlige altid at vurdere risikoen for den registrerede ved behandling af personoplysninger. Disse risikovurderinger er forskellige fra de risikovurderinger, organisationer har gennemført omfattende de risici som organisationen selv står overfor, og som følger af klassisk sikkerhedsarbejde f.eks. ifølge ISO27001. Den dataansvarlige bør opstille nogle kriterier for, hvornår der skal gennemføres risikovurderinger. Det er f.eks. ikke et krav i databeskyttelsesforordningen, at der gennemføres risikovurderinger for alle systemer, der behandler personoplysninger. Kriterierne kan f.eks. tage udgangspunkt i et trusselskatalog. Risikovurderinger foretages ved at identificere trusler mod den registrerede, og efterfølgende estimere sandsynligheden for at truslen materialiserer sig i en sikkerhedshændelse og de deraf følgende konsekvenser for den registrerede. Risikoen fra truslen kan typisk nedbringes gennem foranstaltninger.

Hvis risikoen ikke kan nedbringes, skal den dataansvarlige zoome ind på konsekvenserne ved truslen gennem en konsekvensanalyse. En konsekvensanalyse er dermed en analyse af konsekvenserne af en påtænkt behandlingsaktivitet for den registreredes rettigheder og frihedsrettigheder.

Formålet med konsekvensanalysen er dog helt det samme som risikoanalysen – nemlig at fokusere på, hvordan man bedst muligt kan beskytte de registrerede og deres rettigheder og minimere risikoen ved behandling af personoplysninger. *Eksempler på konsekvenser* for den registrerede kan f.eks. være dødsfald, at den registrerede ikke kan få afgjort en sag på det rette grundlag, at uvedkommende får adgang til oplysninger, som den registrerede ønsker og har ret til at holde fortrolige, og at der opbygges en omfangsrig profil af den registrerede.

Konsekvensanalysen skal sikre, at de rette spørgsmål til beskyttelse af de registreredes garantier bliver stillet på det rette tidspunkt, når man udvikler nye systemer eller ændrer behandlinger i eksisterende systemer.

2. Skala for de registreredes konsekvenser ved behandling

Man kan lave en skala over, hvilke konsekvenser de registrerede kan stå overfor, og anvende denne skala til at vurdere om risikoen er så stor at der bør gennemføres konsekvensanalyser.

Tabel 1: Eksempel på skal over konsekvenser for den registrerede:

Konsekvenser	Kategori	Eksempel
5	Væsentlige fysiske konsekvenser	• Der kan ikke leveres livsvigtig medicin til borgerne og det kan have fatale konsekvenser. • Borgerens liv er i fare, f.eks. ved afsløring af hemmelige adresser for voldsofre eller vidner. • Redningstransport kan ikke iværksættes. • Borgeren må forlade sit hjem.
4	Væsentlige økonomiske eller omdømmemæssige konsekvenser	• Borgeren kan ikke få udbetalt sine ydelser. • Borgeren er afskåret fra at gennemføre økonomiske transaktioner. • Borgerens forbrugspræferencer og psykologiske profil bliver gennemsigtige og udbudt til højestbydende på markedet. • Borgeren kan blive udstillet eller marginaliseret i sit sociale nærmiljø - herunder med betydelig skade på omdømme. Det kan f.eks. ved underretning om familie med omsorgssvigt eller indtagelse af stoffer.

3	Væsentlige IT-sikkerhedsmæssige eller sociale konsekvenser	• Uvedkommende adgang til væsentlige følsomme eller fortrolige oplysninger, f.eks. terminale, seksuelle eller psykiske sygdomme, misbrug af børn, vold i hjemmet eller religiøst betinget adfærd. • Uvedkommende adgang til oplysninger der kan anvendes til identitetstyveri. • Følsomme oplysninger om børn (f.eks. oplysninger om udadreagerende adfærd, vægtproblemer, mobning, læsevanskeligheder eller konflikter med andre børn) videregivet til klassekammerater eller deres forældre
2	Mindre økonomiske, IT-sikkerhedsmæssige eller sociale konsekvenser	• Borgeren kan ikke få et pas til en bestilt og betalt rejse. • Borgeren kan miste kontrol med login til et system eller få login eksponeret for uvedkommende.
1	Ubehag og reduktion af tilliden til digitaliseringen	• Konsekvenserne er – hvor ubehagelige de end er – afgrænset til et psykisk ubehag for den registrerede selv og uden, at der er fysiske, økonomiske eller sociale konsekvenser.
0	Ingen konsekvens	• Ingen konsekvens.

3. Hvornår skal der gennemføres en konsekvensanalyse?

Databeskyttelsesforordningens artikel 35 fastslår, at der skal gennemføres en konsekvensanalyse, når behandlingen af personoplysninger udgør en høj risiko for de registreredes rettigheder. Den "høje risiko" er grundlæggende det eneste kriterie, der skal være opfyldt, for at der skal gennemføres en konsekvensanalyse. Det betyder, at selve karakteren af behandlingen (f.eks. at man går fra on-premise hosting af alle data til cloud) ikke i sig automatisk udløser en konsekvensanalyse, men hvis risikovurderingen viser, at trusler mod den registreredes rettigheder resulterer i høj risiko for, at det går galt, udløser dette en konsekvensanalyse.

Ved vurdering af om risikoen er høj, bør vurderingen foretages af en anden, end den som skal udføre arbejdet med konsekvensanalysen. Ellers vil der være en mulighed for at vurdere risikoen for lavt, for at undgå arbejdet med at gennemføre konsekvensanalysen. Det er generelt god praksis at have funktionsadskillelse.

Kunsten er at fastlægge, *hvornår risikovurderingen resulterer i en så høj risiko, at kravet om en konsekvensanalyse udløses.* Forordningen nævner nogle af de kriterier, som man skal lægge vægt på i artikel 35 (og P91):

- Anvendelse af nye teknologier (stk. 1)
- Behandlingens karakter, omfang, sammenhæng og formål (stk. 1)
- Systematisk og omfattende evaluering af personlige forhold med henblik på profilering (stk. 3)
- Behandling i stort omfang (større end praktiserende læge/advokat, mindst en region) af følsomme oplysninger (A9) og oplysninger om strafbare forhold (A10) (stk. 3)
- Systematisk overvågning af offentlige områder (stk. 3)

EDPB har i WP248 med udgangspunkt i præambelbetragtning 71, 75 og 91 opstillet ni kriterier, som de finder, bør tillægges vægt, når man skal tage stilling til, om det er nødvendigt at lave en konsekvensanalyse.

Disse kriterier for at lave konsekvensanalyse:

- Evaluering og analyse, herunder profilering og forudsigelse af/om den registrerede

- Automatiserede behandlinger med beslutningstagning med betydelig virkning for den registrerede
- Systematisk observering, overvågning eller kontrol af de registrerede, navnlig når de registrerede ikke er klar over overvågningen og/eller ikke kan undgå at være en del af denne
- Når der behandles følsomme oplysninger, oplysninger om strafbare forhold eller fortrolige oplysninger, der udgør en særlig risiko for de registrerede
- Når der sker en omfattende behandling i form af antallet af registrerede eller mængden af data om de enkelte registrerede og i tilknytning hertil behandlingernes varighed, regelmæssighed eller geografiske omfang
- Når data med forskellige formål køres sammen til et nyt formål
- Når der behandles oplysninger om sårbare registrerede (f.eks. børn, ansatte, psykisk syge, asylansøgere, ældre), hvor der er en skævhed i magtfordelingen mellem den registrerede og den dataansvarlige
- Ved innovativ brug af teknologi eller brug af ny teknologi, hvor der lægges vægt på hvilken viden organisationen i forvejen har om teknologien, og hvilken viden der generelt findes om teknologien og dens konsekvenser for de registrerede
- Når behandlingen hindrer de registrerede i at udøve en rettighed eller gøre brug af en tjeneste eller en kontrakt.

Hvis man opfylder to kriterier eller flere, skal man som hovedregel lave en konsekvensanalyse, medmindre der er konkrete holdepunkter for, at der ikke er en høj risiko. Systemer, der er anmeldt til Datatilsynet efter Databeskyttelsesdirektivet (reglerne for Databeskyttelsesforordningen) er ikke omfattet af reglerne om konsekvensanalyse.

Figur 1: Proces for gennemførsel af konsekvensanalyser

4. Eksempler på vurdering af behov for konsekvensanalyse

For at operationalisere brugen af ovenstående, præsenteres nedenfor en række eksempler på vurderinger af, hvornår der bør og ikke bør gennemføres konsekvensanalyser:

1. CASE: En virksomhed laver en ny bilsensor, hvor der kan laves et biometrisk aftryk af brugernes stemmer, således at bilen kan genkende, hvem der fører bilen og kan indrette temperatur, sæde, spejle, musik m.v. herefter. Der sendes jævnligt samples af stemmer fra bilen til producenten med det formål at forbedre teknologien til at genkende stemmer og lave biometriske aftryk. Da der opbygges biometriske profiler af systemets brugere og disse videregives til producenten, bør der gennemføres en konsekvensanalyse.

2. CASE: En organisation foretager vurdering af, om kunder skal gives kredit ved at gennemgå nøgletal fra offentliggjorte regnskaber eller ved at indhente privatøkonomiske oplysninger fra kunderne eller tredjeparter i form af kreditoplysningsbureauer eller oplysninger offentliggjort af den registrerede på sociale medier. Da der er der tale om en omfattende automatiseret profilering af kunderne, der kan have betydelig konsekvens for kunderne, idet der kombineres personoplysninger fra forskellige kilder (herunder oplysninger, som oprindelig behandles til andre formål), bør der gennemføres konsekvensanalyse.

3. CASE: Et supermarked opsætter TV-overvågning i sin butik og på sit lager. TV-overvågningen er på alle områder compliant med lovgivning og praksis med bl.a. varsling af ansatte, skiltning og sletning. Hvis der sker tyveri i en af supermarkedets butikker, deles optagelsen og supplerende oplysninger dels med de andre butikker i kæden og dels med en brancheorganisation. Da overvågningen er fast, dækker et offentligt område, og især da delingen med andre ikke nødvendigvis er meget gennemsigtig for de registrerede, bør der gennemføres en konsekvensanalyse for butikken. Derimod behøver man ikke foretage en konsekvensanalyse for opsætning af overvågning på lageret, idet det udelukkende filmer på butikkens lokalitet og ikke offentlige områder, og videomaterialet ikke er tilgængeligt for andre end butikkens egen ledelse.

4. CASE: Et forsikringsselskab opbevarer oplysninger om kundernes helbred, dels for at fastslå om kunderne kan tegne ulykkes- og sundhedsforsikringer og dels relateret til de konkrete skadesanmeldelser og den tilknyttede sagsbehandling, som foretages af forsikringsselskabet. Ud fra kundernes transaktionshistorik kan måske afledes et sygdomsforløb ligesom et evt. tidsstempel for en forsikringsbegivenhed kan identificere en person. Da der er tale om behandling af følsomme personoplysninger i betydeligt omfang, bør forsikringsselskabet gennemføre en konsekvensanalyse. Databehandling hvor helbredsoplysninger aggregeres eller på anden vis helt kan adskilles fra individet behøver ikke en konsekvensanalyse. Det kan potentielt blive til rigtig mange konsekvensanalyser. Derfor kan det give mening at have en differentieret tilgang samt at investere i at strømline analyseprocessen.

5. CASE: En myndighed får hostet sine e-mail i en international cloudtjeneste med moderselskab udenfor EU, men med datacentre indenfor EU. Der er indgået en lovlig databehandleraftale. Tredjelandsoverførsel kan ikke udelukkes generelt. Myndigheden har organisatoriske foranstaltninger, som sikrer, at der benyttes e-boks til kommunikation af følsomme og fortrolige oplysninger, når der kommunikeres med borgerne. Myndigheden kan imidlertid ikke sikre, at de ikke modtager forskellige følsomme og fortrolige oplysninger fra borgerne i deres almindelige indbakker, ligesom intern kommunikation via mails kan indeholde følsomme og fortrolige oplysninger. Da myndigheden antages at have en omfattende kommunikation med borgerne, og da der må forventes at lande væsentlige mængder af følsomme og fortrolige oplysninger om borgerne i myndighedens mailsystem, bør der gennemføres en konsekvensanalyse.

6. CASE: Flere selvstændige dataansvarlige organisationer ønsker at udarbejde en fælles whistleblowerløsning, som anvendes af de enkelte dataansvarlige. Organisationerne får en leverandør til at lave en fælles løsning. I dette tilfælde behøver hver enkelt selvstændige dataansvarlige ikke at lave hver deres konsekvensanalyse. I stedet kan de lave en fælles konsekvensanalyse eller tiltræde hinandens konsekvensanalyser under forudsætning af, at de anvendes systemet på samme måde. Generelt gælder det, at når der udvikles fælles behandlingsplatforme, hvor der er flere dataansvarlige, er der mulighed for at udarbejde én konsekvensanalyse, jf. præambelbetragtning 92 til databeskyttelsesforordningen.

7. CASE: En myndighed flytter sit proprietære on-premise ESDH-system til et fælles ESDH-system hos en hostingprovider eller cloud-leverandør, som anvendes af en flerhed af forskellige dataansvarlige. Systemet indeholder bl.a. følsomme personoplysninger om udsatte grupper (f.eks. krisecentre). Ved flytningen introduceres der nye trusler i og med, at systemet er en delt ressource, hvor der er flere dataansvarlige, der håndterer brugere. Myndigheden vurderede i deres risikovurdering, at der var en lav sandsynlighed, men højeste konsekvens for de registrerede i tilfælde af brud på sikkerheden. Når det drejer sig om liv, ære og velfærd for de registrerede og dermed høje konsekvenser, vil dette tale for en konsekvensanalyse uanset at sandligheden er lav. Der udarbejdedes derfor en konsekvensanalyse som resulterede i ændringer af organisatoriske foranstaltninger.

Hvis man er i tvivl om, hvorvidt man skal gennemføre en konsekvensanalyse, må det anbefales at gennemføre konsekvensanalysen, da konsekvensanalyser generelt må anses at være et nyttigt redskab til at skabe compliance med databeskyttelseslovgivningen.

5. Hvornår skal man være særligt opmærksom på, om en risikovurdering kan udløse en konsekvensanalyse

I en række situationer kan der være særlige forhold, der taler for at gennemføre en konsekvensanalyse, men uden at man kan fastslå at der altid skal gennemføres en konsekvensanalyse. Nogle af disse særlige forhold illustreres af de nedenstående cases.

8. CASE: En myndighed eller en kommune planlægger – f.eks. som konsekvens af et valg eller en politisk beslutning – en større organisationsændring, hvor direktionsområder nedlægges, medarbejdere flyttes, afdelinger får nye navne, og adgangsrettigheder ændres/flyttes. Ved større organisationsændringer udgør det en særlig risiko, at der henset til behandlingernes karakter, omfang, sammenhæng og formål kan begås fejl. Man skal derfor i sådanne situationer være særligt opmærksom på, om risikovurderingen resulterer i en høj risiko, og i givet fald skal der gennemføres konsekvensanalyser.

9. CASE: Omsorgsområdet ønsker at købe en app-løsning hos en it-leverandør, hvor der er snitflade til kommunens omsorgssystem. Formålet er, at der skal skabes bedre og mere sikker kommunikation med bl.a. pårørende. I appen kan pårørende, hvis borgeren giver tilladelse/fuldmagt, få adgang til afgrænsede dele af borgerens sag, og pårørende kan kommunikere direkte med plejehjemmet. Oplysningerne bliver dermed tilgængelige for personer, som ikke er underlagt professionel tavshedspligt. I løsningen skal der bl.a. håndteres rettigheder til løsningen og dokumentation for tilladelsen. Da der er tale om adgang til følsomme personoplysninger med en ikke ubetydelig sandsynlighed og konsekvenser for de registrerede, men omvendt ikke med risiko for de registreredes liv, skal det overvejes at gennemføre konsekvensanalyse.

10. CASE: En myndighed ønsker at omlægge en afgørelsesproces fra manuel sagsbehandling til automatisk afgørelse – f.eks. en afgørelse af om en borger kvalificerer sig til at modtage en ydelse. Ved omlægningen skal der altid gennemføres konsekvensanalyse.

I praksis anvendes der dog sjældent reelt automatiske afgørelser i databeskyttelsesforordningens forstand. Reelt er der oftest tale om anvendelse af softwarerobotter, som understøtter afgørelsen. I sådanne tilfælde er der ikke krav om at gennemføre konsekvensanalyser, men det bør overvejes, om afgørelsen er så automatiseret, at det bør udløse en konsekvensanalyse.

6. Hvornår skal en konsekvensanalyse IKKE gennemføres?

Når det ikke er krævet af loven i form af "høj risiko" for de registrerede, står det altid den dataansvarlige frit for at beslutte at gennemføre en konsekvensanalyse.

Hvis der er gennemført en konsekvensanalyse i forbindelse med vedtagelsen af et retsgrundlag for behandling, behøver den dataansvarlige ikke gennemføre en konsekvensanalyse (jf. artikel 35, stk. 10). Vi har meget få eksempler på dette, og i alle tilfælde opfylder de ikke formen i artikel 35.

11. CASE: En organisation tilbyder sine medarbejdere en SmartPhone, som kan bruges arbejdsmæssigt såvel som privat. Organisationen kræver, at der er login på telefonen og enforcer det gennem en gruppe-politik. Medarbejderne kan selv vælge, om de vil logge ind med en selvvalgt PIN-kode, eller om de vil slå biometrisk login til. Det biometriske login virker som en matematisk repræsentation af et eller flere af medarbejderens biometriske karakteristika (f.eks. fingeraftryk eller ansigtstræk). Den matematiske repræsentation gemmes lokalt på SmartPhonen i krypteret format i en tamper-resistent hardware chip. Arbejdsgiveren eller producenter af SmartPhonen har ikke adgang til den matematiske repræsentation. Selv om der på SmartPhonen er tale om behandling af følsomme oplysninger (behandling af biometrisk informationer med identifikation som formål), som er omfattet af både EDPBs tjekliste og de nationale tilsyns tjeklister, skal organisationen ikke gennemføre en konsekvensanalyse. Det er ikke organisationen, der instruerer i brugen af biometri til identifikation, og organisationen har ikke adgang til de biometriske data, der behandles på udstyret. Videre er der en risiko for den registrerede for, at den matematiske repræsentation af de(t) biometriske karakteristika eksponeres for uvedkommende, med de teknologiske midler vi kender til i dag, gående mod nul.

12. CASE: En organisation iværksætter en række sikkerhedsforanstaltninger for at beskytte sine kunders personoplysninger og rettigheder. Foranstaltningerne betyder bl.a., at al indgående og udgående netværkstrafik opsnappes og dekrypteres hvis muligt og analyseres og filtreres automatisk i henhold til fastlagte politikker. Tillige opsamles logs fra servere og terminaludstyr og også disse analyseres. Foranstaltningerne er proportionale henset til risikovurderingen, vedtaget i samarbejdsudvalget, der er fastlagt en proportional slettepolitik, og der er sket oplysning og følger i øvrigt på alle måder de persondataretlige regler. Selv om der er tale om en systematisk overvågning, behøver der ikke blive gennemført konsekvensanalyse, hverken set fra de ansattes eller kundernes perspektiv, fordi overvågningen sker til sikkerhedsformål og dermed beskyttelse af de registreredes rettigheder.

13. CASE: En organisation opbygger besøgs- og købsprofiler af kunder på baggrund af besøg på organisationens websted, brug af organisationens app og kundernes øvrige kommunikation med organisationen. På baggrund af denne indsamling opbygges profiler mhp. markedsføring og visning af produkter i prioriteret rækkefølge og fastlæggelse af pris. Der suppleres ikke med oplysninger fra tredjeparter eller oplysninger offentliggjort af den registrerede. I dette tilfælde er der tale om en begrænset profilering med beskeden virkning for den registrerede, og der bør derfor ikke gennemføres konsekvensanalyse. Hvis profileringen bliver omfattende og f.eks. inddrager data fra andre kilder, øges risikoen for den registrerede, og der skal så i givet fald gennemføres en konsekvensanalyse.

14. CASE: En webshop sælger via en dansk hostet hjemmeside dagligvarer til forbrugerne. Kunderne kan kontakte virksomheden via e-mail. E-mail hostes i en international cloudtjeneste med moderselskab udenfor EU, men med datacentre indenfor EU. Der er indgået en lovlig databehandleraftale. Tredjelandsoverførsel kan ikke udelukkes generelt. Da webshoppen alene forventer at behandle almindelige personoplysninger i sin mailkorrespondance med kunderne udgør det ikke nogen særlig risiko for de registrerede, at deres kundehenvendelser via mail hostes af den internationale cloududbyder, og der bør derfor ikke gennemføres konsekvensanalyse.

7. Hvordan gennemføres en konsekvensanalyse?

Som nævnt ovenfor skal der gennemføres en konsekvensvurdering, når risikoen ved en behandling for de registrerede er høj.

Første skridt til at gennemføre konsekvensanalysen er vurderingen af risikoen

Databeskyttelsesforordningens artikel 35, stk. 7 præciserer, at konsekvensanalysen mindst skal omfatte:

- En systematisk beskrivelse af de planlagte behandlingsaktiviteter
- Formålet med behandlingerne, herunder de legitime interesser som evt. forfølges
- En vurdering af om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene
- En vurdering af de registreredes risici
- De foranstaltninger, der påtænkes for at imødegå risici

Konsekvensanalyser kan opfylde ovenstående i forskellige grader af grundighed. Det er vigtigt at have en proportional tilgang til konsekvensanalyser, ellers kan den dataansvarlige i praksis blive overvældet af opgaven. Det må forventes, at jo mindre konsekvenserne for de registrerede er, jo mere enkelt et framework for analysen kan der anvendes.

I praksis kan man sige, at en konsekvensanalyse består af en analyse og en proces. Analysen indebærer, at man får afklaret de rette forhold ved at stille de rette spørgsmål til de rette aktører. Processen sikrer, at man får stillet de rette spørgsmål på det rette tidspunkt i forhold til planlægningen og behandlingen af personoplysninger.

Andet skridt er at vælge sin procesmodel og sin spørgeramme

Spørgerammen: I Bilag 1, findes forslag til en overordnet spørgeramme. Spørgerammen er en slags bruttoliste, hvor relevante spørgsmål kan udvælges til konsekvensanalysen. Ved konkret anvendelse skal spørgerammen kun tage udgangspunkt i de trusler, som der i risikovurderingen udgør en høj risiko. Det er ikke hele risikovurderingen og den samlede behandlingsaktivitet, som der skal udarbejdes en konsekvensanalyse af.

Procesmodel: Der findes mange forskellige procesmodeller for gennemførelse af konsekvensanalyser. I standarden for konsekvensanalyser, som Justitsministeriet henviser til betænkning 1565, ISO29134, findes en meget omfattende procesmodel, hvor alt forberedes og planlægges ned i mindste detalje over en tyve trins model. I EDPB's WP248 findes en mindre kompliceret procesmodel, som anbefaler, at man løber igennem en syv-trins model. I DI's vejledning om konsekvensanalyser anbefales det, at man knytter sin

analyse an til den udviklingsmodel, som organisationen anvender og dermed får de stillet de rigtige spørgsmål på det rette udviklingstrin.

En organisation skal vælge den konsekvensanalysemodel, som passer bedst til organisationen: Hvis det f.eks. passer bedst at nedsætte et konsekvensanalyseboard, som opstiller generelle kriterier for hvornår, hvordan, af og med hvem konsekvensanalyser skal gennemføres, må man gøre det. Man skal dog være opmærksom på, at databeskyttelsesforordningens krav ikke går videre end ovenstående. I nærværende kontekst anbefales det, at man som minimum har følgende trin i konsekvensanalysen:

- Beskriv behandlingen, formålet med behandlingen og hvilke personoplysninger, der indgår i behandlingen
- Fastlæg om behandlingen som beskrevet er nødvendig og proportional
- Fastlæg hvilke konsekvenser behandlingen kan have for de registrerede og inddrag gerne dem eller andre der har viden om deres risici og opfattelse heraf
- Iværksæt mitigerende foranstaltninger, som kan reducere konsekvenserne og den generelle risiko
- Dokumenter analysens resultater og følg op gennem årlige audits at foranstaltningerne fortsat virker

Jo større risiko og konsekvens der er for de registrerede, og jo flere af punkterne i afsnittet "Hvornår…", der er opfyldt, jo større krav må der stilles til den metodik, der anvendes til at gennemføre konsekvensanalysen.

Tredje skridt er at dokumentere og analysere resultatet fra konsekvensanalysen.

Herunder også iværksætte de resultater der er af konsekvensanalysen – f.eks. iværksætte foranstaltninger eller foretage anmeldelse til Datatilsynet, hvis risikoen ikke kan nedbringes.

8. Supplerende betragtninger

Foruden ovenstående betragtninger om hvornår og hvordan konsekvensanalyser gennemføres, er der en række observationer af mere formel karakter, som det kan være relevant at inddrage i sine overvejelser om konsekvensanalyser:

- Det er den dataansvarlige, som er ansvarlig for at fastlægge, hvornår konsekvensanalyser skal gennemføres og for at tilsikre, at de faktisk gennemføres
- Konsekvensanalysen skal gennemføres inden behandlingerne påbegyndes (P90), og opdateres når behandlingen påbegyndes (WP248, p. 17).
- Konsekvensanalysen kan omfatte flere behandlingsaktiviteter (A35, stk. 1 og P92)
- Hvis der er udpeget en DPO, skal vedkommende inddrages i arbejdet med konsekvensanalyse (A35, stk. 2)
- Datatilsynet skal inddrages, hvis der fortsat efter iværksatte mitigerende foranstaltninger, er høj risiko for de registrerede (A36)
- Den dataansvarlige kan indhente synspunkter fra de registrerede i forbindelse med udformningen af konsekvensanalysen. Mere generelt skal den dataansvarlige sikre, at alle relevante parter giver input til udarbejdelse af konsekvensanalysen.
- Der skal ikke obligatorisk foretages konsekvensanalyser af behandlinger, som var anmeldt til Datatilsynet efter databeskyttelsesdirektivet. Reglerne gælder således kun for nye systemer fra efter 25. maj 2018 og systemer, hvortil der er foretaget væsentlige ændringer efter 25. maj 2018.

- Den dataansvarlige skal tage stilling til om hele eller en del af konsekvensanalysen skal offentliggøres.
- Du skal lave en ny konsekvensanalyse, hvis risikobilledet ændrer sig væsentligt.

9. Referencer

EDPBs working paper om konsekvensanalyser, WP248: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Datatilsynets vejledning om konsekvensanalyser:
https://www.datatilsynet.dk/media/6563/konsekvensanalyse.pdf

Datatilsynets liste over behandlinger som medfører behov for konsekvensanalyser:
https://www.datatilsynet.dk/Media/4/1/Datatilsynets%20liste%20over%20behandlinger%20der%20altid%20er%20underlagt%20kravet%20om%20en%20konsekvensanalyse%20(2).pdf

Datatilsynet og Rådet for Digital Sikkerheds vejledning om risikovurdering:
https://www.datatilsynet.dk/media/7697/vejledende-tekst-om-risikovurdering.pdf.

Bilag 1: Konsekvensanalysens spørgeramme

Beskrivelse af behandlingen

- Hvem behandles der oplysninger om? (kategorier af registrerede: f.eks. borgere, børn, sårbare grupper, ansatte og kunder)
- Hvilke typer af personoplysninger behandles der (f.eks. diagnoser, karakterer, medicin, kreditkortnummer og CPR) og hvilken følsomhed har de (f.eks. følsomme, fortrolige, straffedomme eller almindelige)
- Hvilke omstændigheder er der omkring personoplysningerne? (f.eks. antal registrerede, bredde i personoplysninger, antallet af registrerede, systematik i behandlingen (hyppighed, tidsserier) og geografisk bredde)
- Hvilke omstændigheder er der om behandlingen? (f.eks. hvorfra kommer personoplysningerne, hvordan anvendes personoplysningerne (i hvilke systemer og til hvilke beslutninger), hvordan opbevares personoplysningerne, hvem indenfor og udenfor organisationen kan tilgå data, sker der tredjelandsoverførsel og hvad er omstændighederne ved overførslen, hvor længe opbevares data (inden de slettes), anvendes der nye teknologier eller behandlingsformer, anvendes der nye teknologier eller behandlingsformer)
- Har den dataansvarlige erfaring med denne type behandlinger?

Beskrivelse af behandlingens formål

- Hvad er formålene med behandlingen? (f.eks. salg, service, sagsbehandling, afgørelse eller profilering)
- Sker der videre behandling til andre formål (f.eks. forskning, statistik eller dokumentation)
- Hvilket retligt grundlag er der for behandlingen (f.eks. samtykke, kontrakt, retlig forpligtelse, myndighedsudøvelse/samfundets interesse eller interesseafvejning og hvis der behandles følsomme oplysninger er behandlingen så omfattet af en af undtagelserne)
- Hvis legitim interesse anvendes som retligt grundlag for behandling, hvad er den legitime interesse så?
- Hvis samtykke anvendes som retligt grundlag for behandling, hvordan er dette så indhentet? (f.eks. kan det dokumenteres over tid, kan det let trækkes tilbage)
- Hvad er udbyttet med behandlingen for de relevante parter (f.eks. den registrerede modtager en vare eller en ydelse og den dataansvarlige får et salg eller opfylder en forpligtelse)

Behandlingsaktiviteternes nødvendighed og rimelighed

- Kan formålet opnås med mindre indgribende behandling? (f.eks. er det nødvendigt at behandle oplysninger om identificerede personer eller kan man anvende syntetiske data, anonyme data, pseudonyme personoplysninger eller kan man i nogle af behandlingsaktiviteterne begrænse mulighederne for identifikation)
- Hvordan er forholdet mellem den registrerede og den dataansvarlige? (f.eks. tvinges den registrerede til at få sine personoplysninger behandlet eller er behandlingen frivillig, forventer den registrerede behandlingen og har den registrerede særlige forventninger om privatliv)
- Er formålet med behandlingen klart defineret og specifikt?

- Er formålet sagligt og rimeligt? (f.eks. er behandlingen indenfor rammerne af hvad borgerne kan forvente i et demokratisk samfund, er der foretaget en dataetisk analyse eller en vurdering af proportionaliteten af modstående hensyn)
- Kan formålet opnås ved at behandle færre eller undgå at behandle personoplysninger? (f.eks. indsamles der for mange data i bredden med det formål at analysere disse data for at identificere afvigere)
- Sikres det at der altid behandles korrekte personoplysninger? (f.eks. ajourføres personoplysningerne, kan de registrerede berigtige oplysningerne foretages der kvalitetskontrol af behandlede personoplysninger)
- Slettes data, når der henset til formålet ikke længere er behov for at behandle dem? (f.eks. fastlægges slettedato automatisk når data skabes, hvordan håndteres sletningen teknisk og kan man betrygge de registrerede i (og mere generelt dokumentere) at sletning er foretaget)
- Kan man håndtere de registreredes rettigheder? (f.eks. oplysning, ønske om indsigt, sletning, berigtigelse og begrænsning.

Konkretisering af risici og konsekvenser

- Hvilke trusler giver høj risiko for de registrerede? (f.eks. hacking resulterer i at data kommer til uvedkommendes kendskab eller ransomware betyder at data ikke er tilgængelige).
- Hvilke konsekvenser kan disse trusler give anledning til for de registrerede? (f.eks. kan manglende medicinudbringning have fatale konsekvenser for den registrerede eller kan profilering af de registrerede føre til forfølgelse af dem).
- Kan de registrerede synspunkter inddrages? (f.eks. fokusgrupper, interviews eller spørgeskemaer)

Eksisterende og nye mulige mitigerende foranstaltninger

- Hvilke informationsaktiver indgår i behandlingen? (f.eks. cloudtjenester, servere, applikationer, netværksudstyr)
- Hvilke tekniske og organisatoriske sikkerhedsforanstaltninger omfatter de identificerede informationsaktiver? (f.eks. firewall, antivirus, opdatering, logning, data loss prevention, adgangskontrol)
- Hvordan sikres kommunikationen af personoplysninger ind og ud af systemer (f.eks. kryptering eller godkendelse af terminaler, lav evt. en dataflowanalyse)
- Hvilke tekniske og organisatoriske sikkerhedsforanstaltninger er eventuelle databehandlere underlagt (f.eks. krav om ISO27001-certificering eller krav om ISAE3000 eller tilsvarende revisionserklæring)
- Føres der kontrol med eventuelle databehandlere?
- Har de registrerede kontrol over deres personoplysninger? (f.eks. kan de selv bestemme om deres personoplysninger behandles)
- Hvilke muligheder har de registrerede for selv automatisk at udøve deres rettigheder (design af empowerment) (f.eks. har de registrerede selv direkte adgang til deres personoplysninger, har de registrerede direkte adgang til selv at slette personoplysninger)
- Er behandlingen gennemsigtig for de registrerede (f.eks. er de registrerede oplyst om behandlingen)