17/DA

WP 248 rev. 01

Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679

Vedtaget den 4. april 2017

Som senest revideret og vedtaget den 4. oktober 2017.

GRUPPEN VEDRØRENDE BESKYTTELSE AF PERSONER I FORBINDELSE MED BEHANDLING AF PERSONOPLYSNINGER,

som er nedsat ved Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995,

som henviser til artikel 29 og 30 i ovennævnte direktiv, og

som henviser til gruppens forretningsorden,

HAR VEDTAGET FØLGENDE RETNINGSLINJER:

Indholdsfortegnelse

I. Indledning

Forordning (EU) 2016/679[1] (den generelle forordning om databeskyttelse) finder anvendelse fra den 25. maj 2018. Ved forordningens artikel 35 indføres i lighed med direktiv 2016/680[2] begrebet en konsekvensanalyse vedrørende databeskyttelse[3].

En konsekvensanalyse vedrørende databeskyttelse er en proces, der har til formål at beskrive behandlingen, vurdere dens nødvendighed og proportionalitet og bidrage til at håndtere de risici for fysiske personers rettigheder og frihedsrettigheder, som behandlingen af personoplysninger medfører[4], ved at vurdere dem og fastlægge foranstaltninger til at afhjælpe dem. Disse konsekvensanalyser vedrørende databeskyttelse er vigtige redskaber for ansvarlighed, idet de ikke kun hjælper de dataansvarlige med at sikre overensstemmelse med kravene i den generelle forordning om databeskyttelse, men også med at påvise, at der er truffet passende foranstaltninger for at sikre, at forordningen overholdes (se også artikel 24)[5]. Med andre ord er en **konsekvensanalyse vedrørende databeskyttelse en proces, der skal bidrage til at skabe og påvise overensstemmelse**.

I henhold til den generelle forordning om databeskyttelse kan manglende overholdelse af kravene til en konsekvensanalyse vedrørende databeskyttelse føre til, at den kompetente tilsynsmyndighed

---

[1] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).

[2] I artikel 27 i Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger fastslås endvidere, at der er behov for en konsekvensanalyse vedrørende databeskyttelse, når behandling "*sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder*".

[3] Udtrykket "konsekvensanalyse vedrørende beskyttelse af privatlivets fred" (Privacy Impact Assessment, PIA) anvendes ofte i andre sammenhænge om samme begreb.

[4] I den generelle forordning om databeskyttelse defineres begrebet ikke formelt som sådan, men

- det fastsættes i artikel 35, stk. 7, hvad analysen mindst skal indeholde:
    - "*a) en systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen, herunder i givet fald de legitime interesser, der forfølges af den dataansvarlige*
    - *b) en vurdering af, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene*
    - *c) en vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder som omhandlet i stk. 1 og*
    - *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 denne forordning, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser."*
- mens dens betydning og rolle præciseres i betragtning 84 som følger: "*For at fremme overholdelse af denne forordning bør den dataansvarlige, hvor behandlingsaktiviteter sandsynligvis indebærer en høj risiko for fysiske personers rettigheder og frihedsrettigheder, have ansvaret for at foretage en konsekvensanalyse vedrørende databeskyttelse for navnlig at vurdere denne risikos oprindelse, karakter, særegenhed og alvor*".

[5] Se også betragtning 84: "*Resultatet af analysen bør tages i betragtning, når der skal træffes passende foranstaltninger med henblik på at påvise, at behandlingen af personoplysningerne overholder denne forordning*".

pålægger bøder. Hvis der ikke foretages en konsekvensanalyse vedrørende databeskyttelse, når behandlingen er underlagt en sådan (artikel 35, stk. 1, samt stk. 3 og 4), eller hvis den udføres på en forkert måde (artikel 35, stk. 2, samt stk. 7-9), eller den kompetente tilsynsmyndighed ikke høres i tilfælde, hvor dette er obligatorisk (artikel 36, stk. 3, litra e)), kan dette medføre pålæggelse af en administrativ bøde på op til 10 mio. EUR, eller, hvis det drejer sig om en virksomhed, op til 2 % af dens samlede globale omsætning på årsplan i det foregående regnskabsår, såfremt dette beløb er højere.

II. Retningslinjernes anvendelsesområde

I disse retningslinjer er der taget hensyn til:

- erklæring 14/EN WP 218 fra Artikel 29-Gruppen vedrørende Databeskyttelse[6]
- Artikel 29-Gruppen vedrørende Databeskyttelse, "Guidelines on Data Protection Officers 16/EN WP 243[7]
- Artikel 29-Gruppen, "Opinion on Purpose limitation 13/EN WP 203[8]
- internationale standarder[9].

I overensstemmelse med den risikobaserede tilgang, der danner grundlag for den generelle forordning om databeskyttelse, er der ikke krav om at gennemføre en konsekvensanalyse vedrørende databeskyttelse for alle behandlingsaktiviteter. En sådan konsekvensanalyse kræves kun, hvis behandlingen "*sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder*" (artikel 35, stk. 1). For at sikre en konsekvent fortolkning af de omstændigheder, hvor en konsekvensanalyse vedrørende databeskyttelse er obligatorisk (artikel 35, stk. 3), skal de foreliggende retningslinjer først præcisere dette begreb og opstille kriterier for de lister, som databeskyttelsesmyndighederne skal vedtage i henhold til artikel 35, stk. 4.

Ifølge artikel 70, stk. 1, litra e), kan Det Europæiske Databeskyttelsesråd udstede retningslinjer, henstillinger og bedste praksis for at fremme en ensartet anvendelse af forordningen. Formålet med dette dokument er at forberede Det Europæiske Databeskyttelsesråds fremtidige arbejde i den sammenhæng og derfor at præcisere de relevante bestemmelser i den generelle forordning om databeskyttelse med henblik på at hjælpe de dataansvarlige med at overholde lovgivningen og skabe retssikkerhed for dataansvarlige, der skal gennemføre en konsekvensanalyse vedrørende databeskyttelse.

---

[6] Artikel 29-Gruppens erklæring, "Statement 14/EN WP 218 on the role of a risk-based approach to data protection legal frameworks", vedtaget den 30. maj 2014.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] Artikel 29-Gruppens retningslinjer, "Guidelines on Data Protection Officers 16/EN WP 243", vedtaget den 13. december 2016.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] Artikel 29-Gruppens udtalelse, "Opinion 03/2013 on Purpose limitation 13/EN WP 203", vedtaget den 2. april 2013.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] F.eks. ISO 31000: 2009 – Risikoledelse – Principper og vejledning, Den Internationale Standardiseringsorganisation (ISO) ISO/IEC 29134 (projekt), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, Den Internationale Standardiseringsorganisation (ISO).

Disse retningslinjer sigter også mod at fremme udviklingen af:

- en fælles EU-liste over behandlingsaktiviteter, for hvilke en konsekvensanalyse vedrørende databeskyttelse er obligatorisk (artikel 35, stk. 4)
- en fælles EU-liste over behandlingsaktiviteter, for hvilke der ikke kræves en konsekvensanalyse vedrørende databeskyttelse (artikel 35, stk. 5)
- fælles kriterier for metoder til udførelse af en konsekvensanalyse vedrørende databeskyttelse (artikel 35, stk. 5)
- fælles kriterier for bestemmelse af, hvornår tilsynsmyndigheden skal høres (artikel 36, stk. 1)
- henstillinger, der, hvor det er muligt, bygger på erfaringerne fra EU's medlemsstater.

III. Konsekvensanalyse vedrørende databeskyttelse: Værd at vide om forordningen

Den generelle forordning om databeskyttelse kræver, at dataansvarlige træffer passende foranstaltninger med henblik på at sikre og kunne påvise overensstemmelse med forordningen under hensyntagen til bl.a. "risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder" (artikel 24, stk. 1). De dataansvarliges pligt til i visse tilfælde at foretage en konsekvensanalyse vedrørende databeskyttelse skal forstås på baggrund af deres generelle forpligtelse til på passende vis at sikre en hensigtsmæssig styring af risiciene[10] ved behandling af personoplysninger.

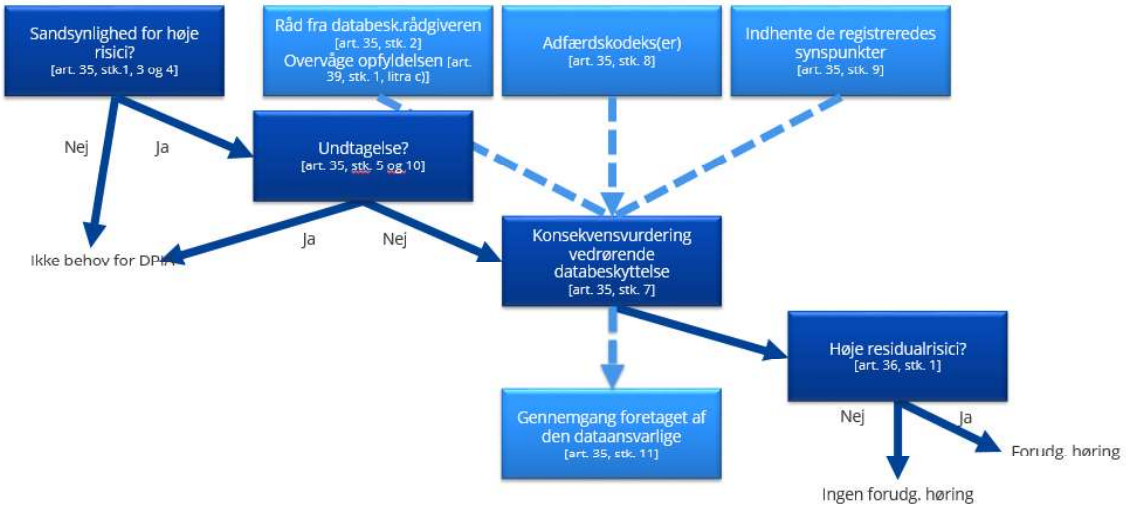
En "risiko" er et scenarie, der beskriver en hændelse og konsekvenserne heraf, som vurderes i forhold til alvor og sandsynlighed. "Risikostyring" kan på den anden side defineres som samordnede aktiviteter vedrørende styring af og kontrol med en organisation med hensyn til risici.

Artikel 35 henviser til "en høj risiko for fysiske personers rettigheder og frihedsrettigheder". Som anført i Artikel 29-Gruppens erklæring om betydningen af en risikobaseret tilgang i de retlige rammer for databeskyttelse vedrører henvisningen til "rettigheder og friheder" for de registrerede først og fremmest retten til databeskyttelse og beskyttelse af privatlivets fred, men kan også omfatte andre grundlæggende rettigheder såsom ytrings- og tankefrihed, fri bevægelighed, forbud mod forskelsbehandling, retten til frihed samt samvittigheds- og religionsfrihed.

I overensstemmelse med den risikobaserede tilgang, der danner grundlag for den generelle forordning om databeskyttelse, er der ikke krav om at gennemføre en konsekvensanalyse vedrørende databeskyttelse for alle behandlingsaktiviteter. Der er i stedet kun krav om en konsekvensanalyse vedrørende databeskyttelse, hvis en bestemt type behandling "sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder" (artikel 35, stk. 1). Den blotte omstændighed, at de forhold, der udløser forpligtelsen til at foretage en konsekvensanalyse vedrørende databeskyttelse, ikke er opfyldt, mindsker dog ikke de dataansvarliges generelle forpligtelse til at træffe hensigtsmæssige foranstaltninger for at styre risiciene for de registreredes rettigheder og frihedsrettigheder. Dette betyder i praksis, at de dataansvarlige løbende skal vurdere de risici, der følger af deres behandlingsaktiviteter, for at identificere de tilfælde, hvor en bestemt type behandling "sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder".

[10] Det skal understreges, at en forudsætning for at styre risiciene for fysiske personers rettigheder og frihedsrettigheder er at få identificeret, analyseret, anslået, evalueret og behandlet (f.eks. afbødet) risiciene samt at revidere dem regelmæssigt. Dataansvarlige kan ikke unddrage sig deres ansvar ved at dække risici med forsikringspolicer.

Følgende figur viser de grundlæggende principper i forbindelse med konsekvensanalysen vedrørende databeskyttelse i den generelle forordning om databeskyttelse:



A. Hvad vedrører en konsekvensanalyse vedrørende databeskyttelse? En enkelt behandlingsaktivitet eller et sæt ensartede behandlingsaktiviteter.

En konsekvensanalyse vedrørende databeskyttelse kan vedrøre en enkelt databehandlingsaktivitet. Det hedder dog i artikel 35, stk. 1: "*En enkelt analyse kan omfatte flere lignende behandlingsaktiviteter, der indebærer lignende høje risici*". Følgende tilføjes i betragtning 92: "*Der kan være tilfælde, hvor det kan være rimeligt og økonomisk at foretage en konsekvensanalyse vedrørende databeskyttelse, som omfatter mere end ét enkelt projekt, f.eks. hvis offentlige myndigheder eller organer har planer om at indføre en fælles applikation eller behandlingsplatform, eller hvis flere dataansvarlige planlægger at indføre en fælles applikation eller behandlingsplatform på tværs af en industrisektor eller et industrisegment eller for en udbredt horisontal aktivitet*".

En enkelt konsekvensanalyse vedrørende databeskyttelse kan bruges til at få adgang til flere behandlingsaktiviteter, der ligner hinanden med hensyn til karakter, omfang, sammenhæng, formål og risici. Konsekvensanalysen vedrørende databeskyttelse har nemlig til formål at sikre en systematisk undersøgelse af nye situationer, som kan føre til en høj risiko for fysiske personers rettigheder og frihedsrettigheder, og det ikke er nødvendigt at foretage en sådan konsekvensanalyse i tilfælde (dvs. behandlingsaktiviteter gennemført i en specifik sammenhæng og med et specifikt formål), der allerede er undersøgt. Dette kan være tilfældet, når der bruges tilsvarende teknologi til at indsamle den samme form for oplysninger til samme formål. F.eks. kan en gruppe kommunale myndigheder, der alle indfører CCTV-systemer, som ligner hinanden, gennemføre en konsekvensanalyse vedrørende databeskyttelse, som dækker behandlingsaktiviteter foretaget af disse særskilte dataansvarlige, eller et jernbaneselskab (enkelt dataansvarlig) kan lade videoovervågning på alle togstationer være omfattet af den samme konsekvensanalyse. Dette kan også anvendes på ensartede behandlingsaktiviteter, som gennemføres af forskellige dataansvarlige. I disse tilfælde bør de implicerede parter være fælles om en referencekonsekvensanalyse, eller den bør gøres offentligt tilgængelig, de foranstaltninger, der er beskrevet i konsekvensanalysen, skal gennemføres, og der skal fremlægges en begrundelse for, at der foretages en enkelt konsekvensanalyse.

Når behandlingsaktiviteten indebærer fælles dataansvarlige, skal de fastlægge deres respektive forpligtelser præcist. Deres konsekvensanalyse vedrørende databeskyttelse bør fastlægge, hvem der

har ansvaret for de forskellige foranstaltninger til behandling af risici og for at beskytte de registreredes rettigheder og frihedsrettigheder. Hver dataansvarlig skal fremlægge sine behov og udveksle nyttige oplysninger uden dog at videregive fortrolige oplysninger (f.eks. beskyttelse af forretningshemmeligheder, intellektuel ejendom eller fortrolige kommercielle oplysninger) eller afsløre sårbarheder.

En konsekvensanalyse vedrørende databeskyttelse kan også være nyttig ved vurderingen af den databeskyttelsesmæssige indvirkning af et teknologiprodukt, f.eks. hardware eller software, i situationer hvor dette sandsynligvis vil blive anvendt af forskellige dataansvarlige til forskellige behandlingsaktiviteter. Naturligvis er den dataansvarlige, der indsætter produktet, stadig forpligtet til at foretage sin egen konsekvensanalyse vedrørende databeskyttelse med hensyn til den konkrete gennemførelse, men denne kan understøttes af en konsekvensanalyse fra produktleverandøren, hvis det er relevant. Et eksempel herpå kan være forholdet mellem producenter af intelligente målere og forsyningsselskaber. Hver produktleverandør eller databehandler bør udveksle nyttige oplysninger uden at videregive forretningshemmeligheder eller skabe sikkerhedsrisici ved at afsløre sårbarheder.

B. Hvilke behandlingsaktiviteter er omfattet af en konsekvensanalyse vedrørende databeskyttelse? Alle behandlingsaktiviteter, der "*sandsynligvis indebærer en høj risiko*", bortset fra visse undtagelser.

I dette afsnit beskrives de situationer, hvor en konsekvensanalyse vedrørende databeskyttelse er obligatorisk, samt de situationer, hvor det ikke er nødvendigt at foretage en sådan.

Medmindre behandlingsaktiviteten er omfattet af en undtagelse (III.B.a), skal der foretages en konsekvensanalyse vedrørende databeskyttelse, når en behandlingsaktivitet "*sandsynligvis indebærer en høj risiko*" (III.B.b).

a) Hvornår er en konsekvensanalyse vedrørende databeskyttelse obligatorisk? Når behandlingsaktiviteten "*sandsynligvis indebærer en høj risiko*".

I den generelle forordning om databeskyttelse kræves det ikke, at der gennemføres en konsekvensanalyse vedrørende databeskyttelse for alle behandlingsaktiviteter, som kan medføre risici for fysiske personers rettigheder og frihedsrettigheder. Det er kun obligatorisk at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis behandlingsaktiviteten "*sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder*" (artikel 35, stk. 1, og artikel 35, stk. 3), suppleret med artikel 35, stk. 4. Det er navnlig relevant, når der indføres ny databehandlingsteknologi[11].

I tilfælde, hvor det ikke er klart, hvorvidt en konsekvensanalyse vedrørende databeskyttelse er påkrævet, anbefaler Artikel 29-Gruppen at gøre det alligevel, da denne analyse er et nyttigt redskab, som kan hjælpe de dataansvarlige med at overholde databeskyttelseslovgivningen.

Selv om en konsekvensanalyse vedrørende databeskyttelse kunne kræves under andre omstændigheder, indeholder artikel 35, stk. 3, nogle eksempler på, hvornår en behandlingsaktivitet "*sandsynligvis vil resultere i store risici*":

- "*a) en systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk behandling, herunder profilering, og som er grundlag for*

[11] Se betragtning 89 og 91 samt artikel 35, stk. 1 og 3, for yderligere eksempler.

afgørelser, der har retsvirkning for den fysiske person eller på tilsvarende vis betydeligt påvirker den fysiske person[12]

- *b) behandling i stort omfang af særlige kategorier af oplysninger, jf. artikel 9, stk. 1, eller af personoplysninger vedrørende straffedomme og lovovertrædelser, jf. artikel 10*[13]*, eller*
- *b) systematisk overvågning af et offentligt tilgængeligt område i stort omfang*".

Som udtrykket "*navnlig"* i første punktum i artikel 35, stk. 3, i den generelle forordning om databeskyttelse viser, skal dette ikke betragtes som en udtømmende liste. Der kan være "højrisikobehandlingsaktiviteter", som ikke er opført på denne liste endnu, men som alligevel indebærer tilsvarende høje risici. Disse behandlingsaktiviteter bør også gøres til genstand for konsekvensanalyser vedrørende databeskyttelse. Derfor er nedenstående kriterier undertiden mere vidtgående end blot en redegørelse for, hvad der skal forstås ved de tre eksempler i artikel 35, stk. 3, i den generelle forordning om databeskyttelse.

For at få et mere konkret sæt behandlingsaktiviteter, som kræver en konsekvensanalyse vedrørende databeskyttelse på grund af deres iboende høje risiko, idet der skal tages hensyn til de særlige elementer i artikel 35, stk. 1, og artikel 35, stk. 3, litra a) - c), bør der i den liste, der skal vedtages på nationalt plan i henhold til artikel 35, stk. 4, og betragtning 71, 75 og 91, i den generelle forordning om databeskyttelse og andre henvisninger heri til behandlingsaktiviteter, der "sandsynligvis vil føre til en høj risiko"[14], tages hensyn til følgende ni kriterier.

1. Evaluering eller analyse, herunder profilering og forudsigelse, især på baggrund af *"forhold vedrørende den registreredes arbejdsindsats, økonomisk situation, helbred, personlige præferencer eller interesser, pålidelighed eller adfærd eller geografiske position eller bevægelser"* (betragtning 71 og 91). Eksempler herpå kan omfatte et finansieringsinstitut, der screener sine kunder mod en referencedatabase eller database over foranstaltninger mod hvidvaskning af penge og finansiering af terrorisme eller over svig, eller en biotekvirksomhed, der tilbyder genetiske tests direkte til forbrugerne for at vurdere og forudsige sygdomme/sundhedsrisici, eller et selskab, der opbygger adfærds- eller markedsføringsprofiler baseret på brugen af dets websted.
2. Automatiseret beslutningstagning med juridisk eller tilsvarende betydelig virkning: behandlingsaktiviteter med sigte på beslutningstagning, der har "*retsvirkning for den fysiske person*" eller "*på tilsvarende vis betydeligt påvirker den fysiske person*" (artikel 35, stk. 3, litra a). Behandlingsaktiviteten kan f.eks. føre til udelukkelse eller forskelsbehandling af enkeltpersoner. Behandlingsaktiviteter med ringe eller ingen påvirkning af enkeltpersoner opfylder ikke dette specifikke kriterium. Yderligere redegørelse for disse begreber vil kunne findes i den kommende vejledning om profilering fra Artikel 29-Gruppen.
3. Systematisk overvågning: behandlingsaktiviteter, der anvendes til at observere, overvåge eller kontrollere registrerede, herunder data indsamlet gennem netværk, eller "*systematisk*

[12] Se betragtning 71: "*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*".

[13] Se betragtning 75: "*hvis 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*".

[14] Se f.eks. betragtning 75, 76, 92 og 116.

overvågning af et offentligt tilgængeligt område" (artikel 35, stk. 3, litra c))[15]. Denne type overvågning er et kriterium, da personoplysningerne kan indsamles under omstændigheder, hvor de registrerede ikke er klar over, hvem der indsamler deres data, og om, hvordan de vil blive anvendt. Derudover kan det være umuligt for den enkelte at undgå at blive genstand for en sådan behandling i et offentligt område (eller offentligt tilgængelige områder).

4. Følsomme oplysninger eller oplysninger af meget personlig karakter: Dette omfatter særlige kategorier af personoplysninger som defineret i artikel 9 (f.eks. oplysninger om enkeltpersoners politiske holdninger) samt personoplysninger vedrørende straffedomme og lovovertrædelser, jf. artikel 10. Et eksempel kan f.eks. være et sygehus, der fører journal over patienterne, eller en privatdetektiv, som opbevarer oplysninger om lovovertrædere. Ud over disse bestemmelser i den generelle forordning om databeskyttelse kan visse kategorier af oplysninger anses for at øge den potentielle risiko for fysiske personers rettigheder og frihedsrettigheder. Disse personoplysninger betragtes som følsomme (i dette udtryks almindelige forstand), fordi de er knyttet til aktiviteter, der henhører under privatlivets fred (såsom elektronisk kommunikation, hvis fortrolighed bør beskyttes), eller fordi de påvirker udøvelsen af en grundlæggende rettighed (såsom data om placering, hvis indsamling sætter spørgsmålstegn ved den frie bevægelighed), eller fordi en overtrædelse heraf tydeligvis indebærer alvorlige konsekvenser for de registreredes dagligdag (f.eks. finansielle data, der kan anvendes til betalingssvig). I den henseende kan det være relevant, om oplysningerne allerede er blevet offentliggjort af den registrerede eller af tredjemand. Det forhold, at personoplysninger er offentligt tilgængelige, kan betragtes som et element, der indgår i vurderingen, hvis oplysningerne forventedes at blive yderligere anvendt til visse formål. Dette kriterium kan også omfatte data såsom personlige dokumenter, e-mails, kalendere og notater fra e-læsere udstyret med notatskrivningsfunktion og meget personlige oplysninger i applikationer til registrering af kropsfunktioner.
5. Oplysninger, der gøres til genstand for omfattende behandling: I den generelle forordning om databeskyttelse defineres det ikke, hvad der forstås ved "omfattende", selv om der findes visse retningslinjer i betragtning 91. Under alle omstændigheder anbefaler Artikel 29-Gruppen, at der især tages hensyn til følgende faktorer, når det vurderes, om der er tale om omfattende behandling[16]:
    a. antal berørte registrerede, enten som et specifikt antal eller som en andel af den relevante population
    b. mængden af data og/eller de forskellige data, der behandles
    c. databehandlingsaktivitetens varighed eller regelmæssighed
    d. databehandlingsaktivitetens geografiske omfang.

[15] Artikel 29-Gruppen fortolker "*systematisk"* som en eller flere af nedenstående (se Artikel 29-Gruppens retningslinjer, Guidelines on Data Protection Officers 16/EN WP 243):

- opstår i henhold til et system
- på forhånd fastlagt, organiseret eller metodisk
- finder sted som led i en generel plan om dataindsamling
- foretages som led i en strategi.

Artikel 29-Gruppen fortolker "offentligt tilgængeligt område" som et sted, der er åbent for ethvert medlem af offentligheden, f.eks. et torv, et indkøbscenter, en gade, en markedsplads, en banegård eller et offentligt bibliotek.

[16] Se Artikel 29-Gruppens retningslinjer, Guidelines on Data Protection Officers 16/EN WP 243.

6. Matching eller kombination af datasæt, f.eks. hidrørende fra to eller flere behandlinger af oplysninger med forskellige formål og/eller foretaget af forskellige dataansvarlige på en måde, som ville overstige den registreredes rimelige forventninger[17].
7. Oplysninger om sårbare registrerede (betragtning 75): Behandlingen af denne type data er et kriterium på grund af den øgede skævhed i magtfordelingen 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 kan omfatte børn (de kan betragtes som værende ude af stand til bevidst og med omtanke at modsætte sig eller give deres samtykke til behandling af deres data), ansatte, mere sårbare udsnit af befolkningen med behov for særlig beskyttelse (psykisk syge personer, asylansøgere, ældre, patienter osv.), og i tilfælde, hvor der kan konstateres ubalance i forholdet mellem den registreredes og den dataansvarliges position.
8. Innovativ brug eller anvendelse af ny teknologi eller nye organisatoriske løsninger, såsom en kombination af brugen af fingeraftryk og ansigtsgenkendelse med henblik på bedre kontrol med fysisk adgang osv. Det fremgår klart af den generelle forordning om databeskyttelse (artikel 35, stk. 1, og betragtning 89 og 91), at brug af ny teknologi, der defineres "*i overensstemmelse med det opnåede niveau af teknologisk viden* " (betragtning 91), kan udløse behovet for en konsekvensanalyse vedrørende databeskyttelse. Dette skyldes, at brug af denne 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. En konsekvensanalyse vedrørende databeskyttelse vil hjælpe dataansvarlige med at forstå og behandle sådanne risici. F.eks. kan visse applikationer inden for "Tingenes Internet" få betydelig indvirkning på borgernes dagligdag og privatlivets fred og derfor kræve en sådan konsekvensanalyse.
9. Når behandlingen i sig selv "*hindrer registrerede i at udøve en rettighed eller gøre brug af en tjeneste eller en kontrakt*" (artikel 22 og betragtning 91). Dette omfatter behandlingsaktiviteter, som sigter mod at tillade, ændre eller afvise de registreredes adgang til en tjeneste eller en kontrakt. Dette gælder f.eks., når en bank screener sine kunder i forhold til en referencedatabase for at beslutte, om de skal tilbydes et lån.

I de fleste tilfælde kan en dataansvarlig antage, at en behandling, der opfylder to kriterier, skal gøres til genstand for en konsekvensanalyse vedrørende databeskyttelse. Generelt mener Artikel 29-Gruppen, at jo flere kriterier en behandling opfylder, jo mere sandsynligt er det, at den udgør en høj risiko for de registreredes rettigheder og frihedsrettigheder og derfor kræver en konsekvensanalyse, uanset de foranstaltninger, som den dataansvarlige agter at træffe.

I nogle tilfælde **kan en dataansvarlig imidlertid antage, at en behandling, der kun opfylder ét af disse kriterier, skal gøres til genstand for en konsekvensanalyse vedrørende databeskyttelse.**

Følgende eksempler illustrerer, hvordan kriterierne bør anvendes til at vurdere, hvorvidt en given behandling kræver en konsekvensanalyse:

[17] Se forklaring i Artikel 29-Gruppens udtalelse, Opinion on Purpose limitation 13/EN WP 203, s. 24.

Eksempler på behandling	Mulige relevante kriterier	Sandsynligt, at der skal foretages en konsekvensanalyse vedrørende databeskyttelse?
Et hospital behandler patienternes genetiske og sundhedsmæssige data (hospitalets informationssystem).	- Følsomme oplysninger eller oplysninger af meget personlig karakter. - Oplysninger om sårbare registrerede. - Oplysninger, der indgår i en omfattende behandling.	Ja
Brugen af et kamerasystem til at overvåge kørselsadfærd på motorveje. Den dataansvarlige påtænker at anvende et intelligent videoanalysesystem til at udvælge bestemte biler og automatisk genkende nummerplader.	- Systematisk overvågning. - Innovativ brug eller anvendelse af teknologiske eller organisatoriske løsninger.	
En virksomhed overvåger systematisk sine ansattes aktiviteter, herunder deres arbejdsplads, internetaktiviteter osv.	- Systematisk overvågning. - Oplysninger om sårbare registrerede.	
Indsamling af data fra offentlige sociale medier til generering af profiler.	- Vurdering eller bedømmelse. - Oplysninger, der indgår i en omfattende behandling. - Matching eller kombination af datasæt. - Følsomme oplysninger eller oplysninger af meget personlig karakter:	
En institution, der opretter en database vedrørende kreditvurdering eller svig på nationalt plan.	- Vurdering eller bedømmelse. - Automatisk beslutningstagning med juridisk eller lignende betydelig virkning. - Hindrer registrerede i at udøve en rettighed eller anvende en tjeneste eller en kontrakt. - Følsomme oplysninger eller oplysninger af meget personlig karakter:	
Oplagring med henblik på arkivering af pseudonymiserede personfølsomme data vedrørende sårbare registrerede i forbindelse med forskningsprojekter eller kliniske forsøg	- Følsomme data. - Oplysninger om sårbare registrerede. - Hindrer registrerede i at udøve en rettighed eller anvende en tjeneste eller en kontrakt.	
"En læges, sundhedspersonales eller en advokats behandling af personoplysninger om patienter eller klienter" (betragtning 91).	- Følsomme oplysninger eller oplysninger af meget personlig karakter. - Oplysninger om sårbare registrerede.	Nej
Et onlinemagasin, der bruger en mailingliste til at sende en generisk daglig oversigt til sine	- Oplysninger, der indgår i en omfattende behandling.	

Eksempler på behandling	Mulige relevante kriterier	Sandsynligt, at der skal foretages en konsekvensanalyse vedrørende databeskyttelse?
abonnenter.		
Et e-handelswebsted, hvis annoncer for dele til veteranbiler involverer begrænset profilering baseret på det, de besøgende har set på eller købt på webstedet.	- Vurdering eller bedømmelse.	

Omvendt kan en behandlingsaktivitet svare til ovennævnte tilfælde, men den dataansvarlige mener alligevel ikke, at den "sandsynligvis vil indebære en høj risiko". I sådanne tilfælde bør den dataansvarlige begrunde og dokumentere begrundelserne for ikke at foretage en konsekvensanalyse og medtage/registrere databeskyttelsesrådgiverens synspunkter.

Desuden fører enhver dataansvarlig som led i princippet om ansvarlighed "*fortegnelser over behandlingsaktiviteter under deres ansvar*", herunder bl.a. formålene med behandlingen, en beskrivelse af kategorierne af personoplysninger og af modtagere af oplysningerne, og "*hvis det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i artikel 32, stk. 1*" (artikel 30, stk. 1) og vurderer, om behandlingen sandsynligvis vil indebære en høj risiko, også selv om de i sidste instans beslutter ikke at foretage en konsekvensanalyse vedrørende databeskyttelse.

NB: Tilsynsmyndigheden udarbejder og offentliggør en liste over de typer af behandlingsaktiviteter, der er underlagt kravet om en konsekvensanalyse vedrørende databeskyttelse til Databeskyttelsesrådet (artikel 35, stk. 4)[18]. Ovennævnte kriterier kan hjælpe tilsynsmyndighederne med at udarbejde en liste, der løbende suppleres med mere specifikt indhold, hvis det er relevant. F.eks. kan behandling af enhver type biometriske oplysninger eller oplysninger om børn også betragtes som relevante i forbindelse med udviklingen af en liste i henhold til artikel 35, stk. 4.

b) Hvornår er en konsekvensanalyse vedrørende databeskyttelse ikke påkrævet? Når det ikke er tilfældet, at behandlingen "*sandsynligvis indebærer en høj risiko*", eller der foreligger en tilsvarende konsekvensanalyse, eller behandlingen er blevet godkendt før maj 2018, eller den har et retsgrundlag, eller den er opført på den liste over behandlingsaktiviteter, for hvilke en konsekvensanalyse ikke er påkrævet.

Artikel 29-Gruppen mener ikke, at en konsekvensanalyse vedrørende databeskyttelse er påkrævet i følgende tilfælde:

- **hvis det ikke kan fastslås, at behandlingen "*sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder*" (artikel 35, stk. 1)**

[18] I denne forbindelse "*anvender den kompetente tilsynsmyndighed den sammenhængsmekanisme, der er omhandlet i artikel 63, hvis sådanne lister omfatter behandlingsaktiviteter, der vedrører udbud af varer eller tjenesteydelser til registrerede eller overvågning af sådanne registreredes adfærd i flere medlemsstater, eller som i væsentlig grad kan påvirke den frie udveksling af personoplysninger i Unionen*" (artikel 35, stk. 6).

- **når behandlingens karakter, omfang, sammenhæng og formål er meget lig den behandling, der er udført en konsekvensanalyse af.** I sådanne tilfælde kan resultaterne af en konsekvensanalyse for en tilsvarende behandling anvendes (artikel 35, stk. 1[19]).
- når behandlingsaktiviteter er blevet kontrolleret af en tilsynsmyndighed før maj 2018 på særlige betingelser, som ikke har ændret sig[20] (se III.C)
- **hvis en behandlingsaktivitet** i henhold til artikel 6, stk. 1, litra c) eller e) **har retsgrundlag** i EU-retten eller medlemsstaternes lovgivning, hvis lovgivningen regulerer den specifikke behandling, og **hvis der allerede er foretaget en konsekvensanalyse vedrørende databeskyttelse** som led i fastlæggelsen af dette retsgrundlag (artikel 35, stk. 10)[21], undtagen hvis en medlemsstat har bestemt, at det er nødvendigt at gennemføre en konsekvensanalyse forud for behandlingsaktiviteterne
- **hvor behandlingen er opført på valgfri liste (udarbejdet af tilsynsmyndigheden) over behandlingsaktiviteter**, for hvilke der ikke kræves nogen konsekvensanalyse (artikel 35, stk. 5). En sådan liste kan indeholde behandlingsaktiviteter, der opfylder de betingelser, som denne myndighed har fastlagt, navnlig i form af retningslinjer, særlige afgørelser eller tilladelser, overensstemmelsesregler osv. (i Frankrig f.eks. tilladelser, undtagelser, forenklede regler, overensstemmelsespakker osv.). Med forbehold af en fornyet vurdering foretaget af den kompetente tilsynsmyndighed er en konsekvensanalyse ikke påkrævet i sådanne tilfælde, men kun hvis behandlingen klart falder inden for rammerne af anvendelsesområdet for den relevante procedure som nævnt i listen og fortsat er i fuld overensstemmelse med alle de relevante krav i den generelle forordning om databeskyttelse.

C. Hvad med allerede eksisterende behandlingsaktiviteter? Konsekvensanalyser vedrørende databeskyttelse er påkrævet i nogle tilfælde.

Kravet om at foretage en konsekvensanalyse finder anvendelse på behandlingsaktiviteter, der sandsynligvis indebærer en høj risiko for fysiske personers rettigheder eller frihedsrettigheder, og for hvilke der er indtruffet en ændring i risiciene, hvor der er taget hensyn til behandlingens karakter, omfang, sammenhæng og formål.

En konsekvensanalyse vedrørende databeskyttelse er ikke nødvendig for behandlingsaktiviteter, der kontrolleres af en tilsynsmyndighed eller databeskyttelsesrådgiveren, jf. artikel 20 i direktiv 95/46/EF, og som gennemføres på en måde, som ikke er ændret siden den forudgående kontrol. Som det hedder i betragtning 171: " *Kommissionsafgørelser og -beslutninger, der er vedtaget i henhold til direktiv 95/46/EF, og tilsynsmyndigheders godkendelser baseret på direktiv 95/46/EF bør fortsat gælde, indtil de ændres, erstattes eller ophæves*".

[19] "*En enkelt analyse kan omfatte flere lignende behandlingsaktiviteter, der indebærer lignende høje risici*".

[20] "*Kommissionsafgørelser og -beslutninger, der er vedtaget i henhold til direktiv 95/46/EF, og tilsynsmyndigheders godkendelser baseret på direktiv 95/46/EF bør fortsat gælde, indtil de ændres, erstattes eller ophæves*" (betragtning 171).

[21] Når der foretages en konsekvensanalyse på det tidspunkt, hvor den lovgivning, der danner retsgrundlag for behandlingen, er under udarbejdelse, er en revision sandsynligvis påkrævet, før behandlingsaktiviteterne igangsættes, da den vedtagne lovgivning kan afvige fra forslaget på en måde, der kan påvirke privatlivets fred og databeskyttelse. Muligvis er der desuden heller ikke adgang til tilstrækkelige tekniske oplysninger om den konkrete behandling på tidspunktet for lovgivningens vedtagelse, heller ikke hvis denne er ledsaget af en konsekvensanalyse vedrørende databeskyttelse. I sådanne tilfælde kan det være nødvendigt at foretage en specifik konsekvensanalyse før de egentlige behandlingsaktiviteter.

Omvendt betyder dette, at enhver databehandling, hvor gennemførelsesbetingelserne (omfang, formål, indsamlede personoplysninger, dataansvarliges eller modtageres identitet, opbevaringsperiode, tekniske og organisatoriske foranstaltninger osv.) er blevet ændret siden den forudgående kontrol foretaget af tilsynsmyndigheden eller af databeskyttelsesrådgiveren, og som sandsynligvis vil indebære en høj risiko, bør gøres til genstand for en konsekvensanalyse vedrørende databeskyttelse.

Desuden kan det være nødvendigt at gennemføre en konsekvensanalyse efter en ændring af de risici, der opstår på grund af behandlingsaktiviteterne[22], f.eks. fordi ny teknologi er taget i brug, eller fordi personoplysninger bruges til et andet formål. Databehandlingsaktiviteter kan udvikle sig hurtigt, og der kan opstå nye sårbarheder. Derfor bør det bemærkes, at revisionen af en konsekvensanalyse ikke kun er nyttig med henblik på løbende forbedringer, men også kritisk for at bevare et højt databeskyttelsesniveau i et miljø, der ændrer sig over tid. En konsekvensanalyse vedrørende databeskyttelse kan også blive nødvendig, hvis den organisatoriske eller samfundsmæssige sammenhæng har ændret sig, f.eks. fordi virkningerne af visse automatiserede afgørelser er blevet større, eller hvis nye kategorier af registrerede bliver udsat for forskelsbehandling. Hvert af disse eksempler kan være et element, der fører til en ændring af den risiko, der følger af den pågældende behandlingsaktivitet.

Omvendt kan visse ændringer også mindske risikoen. F.eks. kan en behandlingsaktivitet udvikle sig, således at beslutningerne ikke længere træffes automatisk, eller hvis en overvågningsaktivitet ikke længere er systematisk. I så fald kan revisionen af risikoanalysen godtgøre, at det ikke længere er nødvendigt at foretage en konsekvensanalyse vedrørende databeskyttelse.

I overensstemmelse med god praksis **bør en konsekvensanalyse vedrørende databeskyttelse løbende revideres og regelmæssigt revurderes.** Selv hvis der ikke er krav om en konsekvensanalyse vedrørende databeskyttelse pr. 25. maj 2018, skal den dataansvarlige foretage en sådan som led i sine generelle forpligtelser vedrørende ansvarlighed.

D. Hvordan foretages en konsekvensanalyse vedrørende databeskyttelse?

a) På hvilket tidspunkt bør en konsekvensanalyse vedrørende databeskyttelse foretages? Forud for behandlingen.

Konsekvensanalysen for databeskyttelse bør foretages "*forud for behandlingen"* (artikel 35, stk. 1, og artikel 35, stk. 10, betragtning 90 og 93)[23]. Dette er i overensstemmelse med principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger (artikel 25 og betragtning 78). Konsekvensanalysen vedrørende databeskyttelse bør ses som et redskab til at hjælpe beslutningsprocessen vedrørende behandlingen.

Konsekvensanalysen vedrørende databeskyttelse bør indledes så tidligt som muligt i udformningen af behandlingsaktiviteten, selv om nogle af bearbejdningsprocesserne stadig er ukendte. Ajourføring af

[22] For så vidt angår sammenhængen, de indsamlede data, formål, funktioner, behandlede personoplysninger, modtagere, datakombinationer, risici (underliggende aktiver, risikokilder, potentielle virkninger, trusler osv.), sikkerhedsforanstaltninger og internationale overførsler.

[23] Undtagen når der er tale om en igangværende behandling, som tilsynsmyndigheden har foretaget forudgående kontrol af, hvor konsekvensanalysen vedrørende databehandling bør gennemføres, inden der foretages betydelige ændringer.

konsekvensanalysen vedrørende databeskyttelse gennem projektets levetid vil sikre, at der tages hensyn til databeskyttelse og privatlivets fred, og vil tilskynde til etablering af løsninger, der fremmer overholdelsen. Det kan også være nødvendigt at gentage de enkelte skridt i vurderingen, efterhånden som udviklingen skrider frem, da udvælgelsen af visse tekniske eller organisatoriske foranstaltninger kan påvirke alvoren af eller sandsynligheden for de risici, der er forbundet med behandlingen.

Den omstændighed, at konsekvensanalysen vedrørende databeskyttelse skal ajourføres, så snart behandlingen reelt er indledt, udgør ikke en gyldig begrundelse for at udskyde eller undlade at foretage en konsekvensanalyse vedrørende databeskyttelse. Konsekvensanalysen vedrørende databeskyttelse er en løbende proces, navnlig når behandlingsoperationen er dynamisk og ændres løbende. **Gennemførelsen af en konsekvensanalyse for databeskyttelse er en løbende proces, ikke en engangsforeteelse**.

b) Hvem er forpligtet til at udføre konsekvensanalysen vedrørende databeskyttelse? Den dataansvarlige sammen med databeskyttelsesrådgiveren og databehandleren.

Den dataansvarlige er ansvarlig for at sikre, at konsekvensanalysen vedrørende databeskyttelse foretages (artikel 35, stk. 2). Konsekvensanalysen vedrørende databeskyttelse kan foretages af en anden person i eller uden for organisationen, men den dataansvarlige bærer det endelige ansvar for denne opgave.

Den dataansvarlige skal også rådføre sig med databeskyttelsesrådgiveren, når en sådan er udpeget (artikel 35, stk. 2), og denne rådgivning og de afgørelser, der træffes af den dataansvarlige, skal dokumenteres i konsekvensanalysen vedrørende databeskyttelse. Databeskyttelsesrådgiveren bør også overvåge udførelsen af konsekvensanalysen vedrørende databeskyttelse (artikel 39, stk. 1, litra c)). Yderligere vejledning findes i Artikel 29-Gruppens "Retningslinjer for databeskyttelsesrådgivere" ("Guidelines on Data Protection Officers", 16/EN, WP 243).

Hvis behandlingen helt eller delvis foretages af en databehandler, **bør databehandleren bistå den dataansvarlige med udførelsen af konsekvensanalysen vedrørende databeskyttelse** og fremlægge alle nødvendige oplysninger (i overensstemmelse med artikel 28, stk. 3, litra f)).

Den dataansvarlige "*indhenter de registreredes eller deres repræsentanters synspunkter"* (artikel 35, stk. 9), "*hvis det er relevant"*. Artikel 29-Gruppen mener, 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. Det skal imidlertid bemærkes, at samtykke til behandling naturligvis ikke er en metode til at indhente synspunkter fra de registrerede
- hvis den dataansvarliges endelige afgørelse afviger fra de registreredes synspunkter, skal dennes begrundelse for at gå videre eller ikke dokumenteres
- den dataansvarlige også bør dokumentere sin begrundelse for ikke at høre de registrerede, hvis denne beslutter, at dette ikke er relevant, f.eks. hvis dette ville skade fortroligheden i forbindelse med virksomheders forretningsplaner eller være uforholdsmæssigt eller uigennemførligt.

Endelig er det god praksis at definere og dokumentere andre specifikke roller og ansvarsområder afhængigt af interne politikker, processer og regler, f.eks.:

- når særlige afdelinger kan tilbyde at udføre en konsekvensanalyse vedrørende databeskyttelse, bør disse afdelinger levere input til konsekvensanalysen vedrørende databeskyttelse og inddrages i valideringsprocessen for konsekvensanalysen vedrørende databeskyttelse
- det anbefales i givet fald at søge rådgivning fra uafhængige eksperter fra forskellige fagområder[24] (advokater, IT-eksperter, sikkerhedseksperter, sociologer, etikere osv.).
- rollerne og ansvarsområderne for databehandlerne skal defineres kontraktligt og konsekvensanalysen vedrørende databeskyttelse skal udføres med databehandlerens hjælp under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren (artikel 28, stk. 3, litra f))
- den ansvarlige for informationssikkerhed, hvis en sådan er udpeget, og databeskyttelsesrådgiveren kan foreslå, at den dataansvarlige foretager en konsekvensanalyse vedrørende databeskyttelse for en specifik behandlingsoperation, og skal hjælpe de berørte parter med metodologien, hjælpe med at evaluere kvaliteten af risikovurderingen, og vurderingen af, hvorvidt residualrisikoen er acceptabel, samt med at udvikle viden, der er specifik for den dataansvarliges situation
- den ansvarlige for informationssikkerhed, hvis en sådan er udpeget, og/eller IT-afdelingen skal yde bistand til den dataansvarlige og kan foreslå, at der foretages en konsekvensanalyse vedrørende databeskyttelse for en specifik behandlingsaktivitet afhængigt af de sikkerhedsmæssige eller operationelle behov.

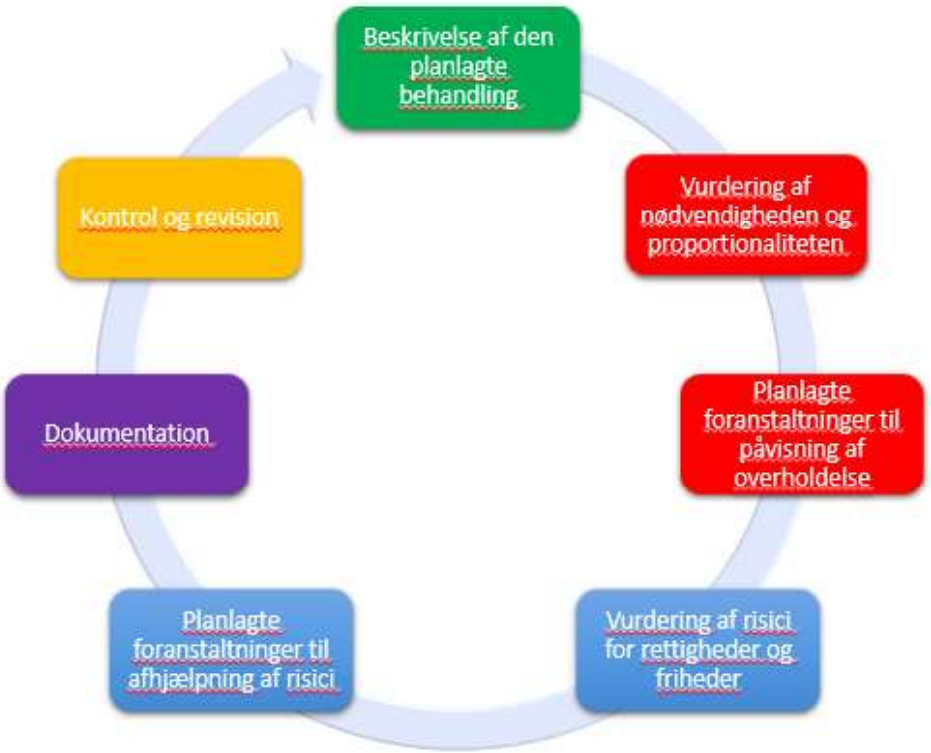
c) Hvilken metodologi bruger man til at foretage en konsekvensanalyse vedrørende databeskyttelse? Forskellige metodologier, men fælles kriterier.

[24] *Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

I den generelle forordning om databeskyttelse fastsættes der minimumskrav for en konsekvensanalyse vedrørende databeskyttelse (artikel 35, stk. 7, og betragtning 84 og 90):

- "*en systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen*"
- "*en systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen*"
- "*en vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder*"
- "*de foranstaltninger, der påtænkes for at:*
    - "*imødegå disse risici*"
    - "*påvise overholdelse af denne forordning*".

Den følgende figur viser den generiske iterative proces for udførelse af en konsekvensanalyse vedrørende databeskyttelse[25]:



Overholdelse af godkendte adfærdskodekser (artikel 40) inddrages behørigt (artikel 35, stk. 8) ved vurderingen af konsekvenserne af behandlingsaktiviteterne. Dette kan være nyttigt for at påvise, at man har valgt eller truffet passende foranstaltninger, forudsat at adfærdskodeksen er hensigtsmæssig for behandlingsaktiviteten. Certificeringsmekanismer for databeskyttelse samt databeskyttelsesmærkninger og -mærker med henblik på at påvise, at dataansvarliges og

[25] Det skal understreges, at den her beskrevne proces er iterativ: I praksis er det sandsynligt, at hvert trin gennemgås flere gange, før konsekvensanalysen vedrørende databeskyttelse kan færdiggøres.

databehandleres behandlingsaktiviteter er i overensstemmelse med den generelle forordning om databeskyttelse (artikel 42), samt bindende virksomhedsregler bør også tages i betragtning.

Alle de relevante krav, der er fastsat i den generelle forordning om databeskyttelse, giver en bred, generisk ramme for udformning og gennemførelse af en konsekvensanalyse vedrørende databeskyttelse. Den praktiske gennemførelse af en konsekvensanalyse vedrørende databeskyttelse vil afhænge af de krav, der er fastsat i den generelle forordning om databeskyttelse, som kan suppleres med mere detaljeret praktisk vejledning. Gennemførelsen af konsekvensanalysen vedrørende databeskyttelse er dermed også skalerbar. Dette betyder, at selv mindre dataansvarlige kan udforme og gennemføre en konsekvensanalyse vedrørende databeskyttelse, der passer til deres behandlingsaktiviteter.

Betragtning 90 i den generelle forordning om databeskyttelse indeholder en række elementer i konsekvensanalysen vedrørende databeskyttelse, som overlapper med veldefinerede elementer i risikostyring (f.eks. ISO 31000[26]). Udtrykt i risikostyringsterminologi sigter en konsekvensanalyse vedrørende databeskyttelse mod at "styre risici" for fysiske personers rettigheder og frihedsrettigheder ved hjælp af følgende processer og ved at:

- fastslå sammenhængen: "*under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål samt risikokilderne*"
- vurdere risiciene: "*vurdere den høje risikos specifikke sandsynlighed og alvor*"
- behandle risiciene: "*begrænsning af denne risiko*", "*sikring af beskyttelsen af personoplysninger*" og "*påvisning af overholdelse af denne forordning*".

NB: Konsekvensanalysen vedrørende databeskyttelse i henhold til den generelle forordning om databeskyttelse er et redskab til styring af risici for de registreredes rettigheder og tager således deres perspektiv, som det er tilfældet inden for visse områder (f.eks. samfundssikkerhed). Omvendt fokuserer risikostyringen på andre områder (f.eks. informationssikkerhed) på organisationen.

Den generelle forordning om databeskyttelse giver de datadataansvarlige fleksibilitet til at fastlægge den nøjagtige struktur og form af konsekvensanalysen vedrørende databeskyttelse med henblik på at kunne tilpasse den til den eksisterende arbejdspraksis. Der findes en række forskellige etablerede processer inden for EU og på verdensplan, som tager hensyn til de elementer, der beskrives i betragtning 90. Men uanset formen skal en konsekvensanalyse vedrørende databeskyttelse være en egentlig vurdering af risici, der gør det muligt for de dataansvarlige at træffe foranstaltninger for at afhjælpe dem.

Forskellige metoder (eksempler på metoder for konsekvensanalyser vedrørende beskyttelse af privatlivets fred og vedrørende databeskyttelse findes i bilag 1) kan bruges som hjælp ved gennemførelsen af de grundlæggende krav, der er fastsat i den generelle forordning om databeskyttelse. For at sikre, at disse forskellige tilgange kan eksistere, samtidig med at de dataansvarlige overholder den generelle forordning om databeskyttelse, har man identificeret fælles kriterier (se bilag 2). De præciserer de grundlæggende krav i forordningen, men giver tilstrækkelige muligheder for forskellige former for gennemførelse. Disse kriterier kan anvendes til at påvise, at en bestemt metodologi for konsekvensanalysen vedrørende databeskyttelse opfylder de standarder, der

[26] Risk management processes: communication and consultation, establishing the context, risk assessment, risk treatment, monitoring and review (se terminologi og definitioner samt indholdsfortegnelse i ISO 31000-oversigten: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

kræves i henhold til den generelle forordning om databeskyttelse. **Det er op til den dataansvarlige at vælge en metode, men den skal være i overensstemmelse med kriterierne i bilag 2**.

Artikel 29-Gruppen tilskynder til udvikling af sektorspecifikke rammer for konsekvensanalyser vedrørende databeskyttelse. Dette skyldes, at de kan trække på sektorspecifik viden, hvilket betyder, at konsekvensanalysen vedrørende databeskyttelse kan rettes mod de nærmere detaljer ved en bestemt type behandlingsaktivitet (f.eks.: bestemte typer data, virksomhedsaktiver, potentielle virkninger, trusler, foranstaltninger). Dette betyder, at konsekvensanalysen vedrørende databeskyttelse kan afhjælpe de problemer, der opstår i en bestemt økonomisk sektor, eller ved anvendelse af bestemte teknologier eller udførelse af bestemte typer behandlingsaktiviteter.

Endelig foretager den dataansvarlige, hvis det er nødvendigt, "*en fornyet gennemgang for at vurdere, hvorvidt behandling er foretaget i overensstemmelse med konsekvensanalysen vedrørende databeskyttelse, i hvert fald når der er en ændring af den risiko, som behandlingsaktiviteterne udgør*" (artikel 35, stk. 11[27]).

d) Er det obligatorisk at offentliggøre konsekvensanalysen vedrørende databeskyttelse? Nej, men offentliggørelse af et resumé kan fremme tilliden, og hele konsekvensanalysen vedrørende databeskyttelse skal indsendes til tilsynsmyndigheden i tilfælde af forudgående høring eller på anmodning af databeskyttelsesmyndigheden.

Offentliggørelse af konsekvensanalysen vedrørende databeskyttelse er ikke et retligt krav i den generelle forordning om databeskyttelse. Det er den dataansvarliges beslutning, om dette skal gøres. Men de dataansvarlige bør som minimum overveje at offentliggøre dele af konsekvensanalysen eller et resumé af deres konsekvensanalyse vedrørende databeskyttelse.

Formålet med en sådan procedure ville være at bidrage til at skabe tillid til dataansvarliges behandlingsaktiviteter samt at udvise ansvarlighed og gennemsigtighed. Det er navnlig god praksis at offentliggøre en konsekvensanalyse vedrørende databeskyttelse, når offentligheden er berørt af behandlingsaktiviteten. Dette kan navnlig være tilfældet, når en offentlig myndighed foretager en konsekvensanalyse vedrørende databeskyttelse.

Den offentliggjorte konsekvensanalyse vedrørende databeskyttelse behøver ikke at indeholde den samlede vurdering, navnlig når konsekvensanalysen vedrørende databeskyttelse kan indeholde specifikke oplysninger om sikkerhedsrisici for den dataansvarlige eller afsløre forretningshemmeligheder eller kommercielt følsomme oplysninger. I sådanne tilfælde kan den offentliggjorte udgave bestå af et sammendrag af de vigtigste resultater i konsekvensanalysen vedrørende databeskyttelse eller blot en erklæring om, at der er foretaget en konsekvensanalyse vedrørende databeskyttelse.

Når en konsekvensanalyse vedrørende databeskyttelse afslører store residualrisici, skal den dataansvarlige desuden høre tilsynsmyndigheden inden behandling (artikel 36, stk. 1). Som led i denne proces skal hele konsekvensanalysen vedrørende databeskyttelse fremlægges (artikel 36, stk. 3, litra e)). Tilsynsmyndigheden kan yde rådgivning[28] og vil ikke afsløre forretningshemmeligheder eller

[27] I artikel 35, stk. 10, udelukkes kun anvendelsen af artikel 35, stk. 1-7, udtrykkeligt.

[28] Der er kun behov for skriftlig rådgivning af den dataansvarlige, når tilsynsmyndigheden er af den opfattelse, at den planlagte behandling ikke er i overensstemmelse med forordningen, jf. artikel 36, stk. 2.

sikkerhedsbrister med forbehold af de gældende principper for aktindsigt i offentlige dokumenter i de enkelte medlemsstater.

E. Hvornår skal tilsynsmyndigheden høres? Når residualrisiciene er høje.

Som forklaret ovenfor:

- En konsekvensanalyse vedrørende databeskyttelse er påkrævet, når en behandling "*sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder*" (artikel 35, stk. 1, jf. III.B.a). Som eksempel kan nævnes, at behandling af helbredsoplysninger i stort omfang skønnes at ville medføre en høj risiko og kræver en konsekvensanalyse vedrørende databeskyttelse.
- Derefter er det op til den dataansvarlige at vurdere risiciene for de registreredes rettigheder og frihedsrettigheder og at identificere de påtænkte foranstaltninger[29] til at begrænse disse risici til et acceptabelt niveau og at påvise overensstemmelse med den generelle forordning om databeskyttelse (artikel 35, stk. 7, jf. III.C.c). Et eksempel kunne være anvendelse af passende tekniske og organisatoriske sikkerhedsforanstaltninger ved lagring af personoplysninger på bærbare computere (effektiv kryptering af hele harddisken, robust nøgleforvaltning, passende adgangskontrol, sikrede sikkerhedskopier osv.) som supplement til de eksisterende politikker (meddelelse, samtykke, retten til aktindsigt, retten til at gøre indsigelse osv.).

I ovenstående eksempel med bærbare computere gælder det, at hvis den dataansvarlige mener, at risiciene er blevet tilstrækkeligt reduceret, og i henhold til artikel 36, stk. 1, og betragtning 84 og 94, kan behandlingen indledes uden høring af tilsynsmyndigheden. Det er i de tilfælde, hvor den dataansvarlige ikke kan afhjælpe de identificerede risici på fyldestgørende vis (dvs. residualrisiciene fortsat er høje), at den dataansvarlige skal høre tilsynsmyndigheden.

Et eksempel på en uacceptabelt høj residualrisiko omfatter tilfælde, hvor de registrerede kan udsættes for betydelige eller endog uoprettelige konsekvenser, som de muligvis ikke kan overvinde (f.eks.: uretmæssig adgang til data, som kan føre til en trussel mod de registreredes liv, afskedigelse, økonomisk tab), og/eller når det virker indlysende, at risikoen vil indtræffe (f.eks.: når det ikke er muligt at begrænse antallet af personer, der har adgang til dataene på grund af de anvendte metoder til udveksling, anvendelse eller distribution, eller når en velkendt sårbarhed ikke afhjælpes).

Når den dataansvarlige ikke kan finde tilstrækkelige foranstaltninger til at begrænse risiciene til et acceptabelt niveau (dvs. residualrisiciene stadig er høje) skal tilsynsmyndigheden høres[30].

Desuden skal den dataansvarlige høre tilsynsmyndigheden, når medlemsstaternes lovgivning kræver, at dataansvarlige hører og/eller får forudgående godkendelse fra tilsynsmyndigheden i forbindelse med en dataansvarligs behandling med henblik på udførelsen af en opgave i samfundets interesse, herunder behandling i forbindelse med social sikring og folkesundhed (artikel 36, stk. 5).

[29] Dette sker under hensyntagen til de eksisterende retningslinjer fra Det Europæiske Databeskyttelsesråd og tilsynsmyndighederne og under hensyntagen til det aktuelle tekniske niveau og gennemførelsesomkostningerne som foreskrevet i artikel 35, stk. 1.

[30] NB: "*pseudonymisering og kryptering af personoplysninger*" (samt dataminimering, kontrolmekanismer osv.) er ikke nødvendigvis egnede foranstaltninger. De er kun eksempler. De passende foranstaltninger afhænger af sammenhængen og de risici, der er specifikke for behandlingsaktiviteterne.

Det skal imidlertid præciseres, at uanset om der kræves høring af tilsynsmyndigheden på grund af residualrisikoens omfang eller ej, gælder forpligtelsen til at opbevare konsekvensanalysen vedrørende databeskyttelse og i givet fald fortsat at ajourføre den.

IV. Konklusion og anbefalinger

Konsekvensanalyser vedrørende databeskyttelse er et nyttigt redskab for dataansvarlige til at sikre, at der indføres databehandlingssystemer, der er i overensstemmelse med den generelle forordning om databeskyttelse, og de kan være obligatoriske for visse typer behandlingsaktiviteter. De er skalerbare og kan antage forskellige former, men i den generelle forordning om databeskyttelse fastlægges de grundlæggende krav til en effektiv konsekvensanalyse vedrørende databeskyttelse. De dataansvarlige bør betragte gennemførelsen af en konsekvensanalyse vedrørende databeskyttelse som en nyttig og positiv aktivitet, der bidrager til overholdelse af lovgivningen.

I artikel 24, stk. 1, beskrives den dataansvarliges grundlæggende ansvar for overholdelse af den generelle forordning om databeskyttelse: "*Under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning. Disse foranstaltninger skal om nødvendigt revideres og ajourføres*".

Konsekvensanalysen vedrørende databeskyttelse er et centralt element i overholdelsen af forordningen, når der planlægges eller foretages databehandling med høj risiko. Dette betyder, at de dataansvarlige bør anvende de kriterier, der opstilles i dette dokument, til at afgøre, hvorvidt der skal foretages en konsekvensanalyse vedrørende databeskyttelse. Denne liste kan udvides ud over de retlige krav i den generelle forordning om databeskyttelse som følge af interne politikker hos de dataansvarlige. Dette bør resultere i større tillid hos de registrerede og andre dataansvarlige.

Når der planlægges behandlingsaktiviteter, der indebærer en høj risiko, skal den dataansvarlige:

- vælge en metode til konsekvensanalysen vedrørende databeskyttelse (eksempler i bilag 1), som opfylder kriterierne i bilag 2, eller specificere og gennemføre en systematisk procedure for konsekvensanalysen vedrørende databeskyttelse, som:
  - er i overensstemmelse med kriterierne i bilag 2
  - integreres i eksisterende revisionsprocedurer vedrørende udformning, udvikling, ændring, risikostyring og drift i overensstemmelse med interne procedurer og den interne baggrund og kultur
  - inddrager relevante interesserede parter og klart definerer deres ansvar (den dataansvarlige, databeskyttelsesrådgiveren, de registrerede eller deres repræsentanter, erhvervslivet, tekniske tjenester, databehandlere, den ansvarlige for IT-sikkerhed osv.)
- forelægge rapporten om konsekvensanalysen vedrørende databeskyttelse for den kompetente tilsynsmyndighed, når dette kræves
- høre tilsynsmyndigheden, når det ikke er lykkedes den dataansvarlige at fastlægge tilstrækkelige foranstaltninger til at afbøde store risici
- regelmæssigt gennemgå konsekvensanalysen vedrørende databeskyttelse og de behandlingsaktiviteter, som vurderes i denne, som minimum når der sker en ændring af risikoen ved behandlingen af aktiviteten
- dokumentere de trufne afgørelser.

Bilag 1 – Eksempler på eksisterende rammer for konsekvensanalyser vedrørende databeskyttelse i EU

I den generelle forordning om databeskyttelse præciseres det ikke, hvilken procedure for konsekvensanalysen vedrørende databeskyttelse, man skal følge, men i stedet gives de dataansvarlige mulighed for at indføre en ramme, der supplerer deres eksisterende arbejdspraksis, under forudsætning af at der tages hensyn til de komponenter, der findes beskrevet i artikel 35, stk. 7. En sådan ramme kan være skræddersyet til den dataansvarlige eller være fælles for en bestemt branche. Tidligere offentliggjorte rammer, som er udviklet af EU's databeskyttelsesmyndigheder, og sektorspecifikke rammer i EU omfatter f.eks. (listen er ikke udtømmende):

Eksempler på generelle rammer i EU:

- DE: Standard Data Protection Model, V.1.0 – Trial version, 2016[31].
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Impacto Evaluación de una Guía para la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos "(AGPD), 2014.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/node/15798
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Eksempler på EU's sektorspecifikke rammer:

- Ramme for konsekvensvurderinger vedrørende privatlivs- og databeskyttelse i forbindelse med RFID-anvendelser[32].
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_da.pdf
- Modellen for konsekvensanalyser for databeskyttelse i forbindelse med intelligente net og intelligente målersystemer[33]

---

[31] Enstemmigt og udtrykkeligt godkendt (Bayern undlod at stemme) på den 92. konference for forbundsstatens og delstaternes uafhængige databeskyttelsesmyndigheder i Kühlungsborn den 9.-10. november 2016.

[32] Se også:

- Kommissionens henstilling af 12. maj 2009 om gennemførelse af principperne om beskyttelse af personoplysninger og privatlivets fred i forbindelse med anvendelse af radiofrekvensbaseret identifikation.
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Udtalelse 9/2011 om industriens reviderede forslag til en ramme for konsekvensvurderinger vedrørende privatlivs- og databeskyttelse i forbindelse med RFID-anvendelser.
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_da.pdf

[33] Udtalelse nr. 7/2013 om modellen for konsekvensanalyser for databeskyttelse i forbindelse med intelligente net og intelligente målersystemer ("DPIA-modellen") udarbejdet af ekspertgruppe 2 under Kommissionens taskforce for intelligente net. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_da.pdf

http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

En international standard vil også udstikke retningslinjer for, hvilke metoder der skal anvendes for at foretage en konsekvensanalyse vedrørende databeskyttelse (ISO/IEC 29134[34]).

[34] ISO/IEC 29134 (projekt), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, Den Internationale Standardiseringsorganisation (ISO).

Bilag 2 – Kriterier for en acceptabel konsekvensanalyse vedrørende databeskyttelse

Artikel 29-Gruppen foreslår følgende kriterier, som dataansvarlige kan anvende til at vurdere, om en konsekvensanalyse eller en metode til udførelse af en sådan er tilstrækkeligt omfattende til at overholde den generelle forordning om databeskyttelse:

- ☐ Der udarbejdes en systematisk beskrivelse af behandlingsaktiviteterne (artikel 35, stk. 7, litra a)):
  - ☐ Der tages hensyn til behandlingens karakter, omfang, sammenhæng og formål (betragtning 90).
  - ☐ Personoplysninger, modtagere og det tidsrum, personoplysningerne opbevares i, registreres.
  - ☐ Der udarbejdes en funktionel beskrivelse af behandlingsaktiviteten.
  - ☐ De aktiver, som personoplysningerne er afhængige af (hardware, software, netværk, personer, papir eller papirforsendelseskanaler), identificeres.
  - ☐ Der tages hensyn til overholdelse af godkendte adfærdskodekser (artikel 35, stk. 8).
- ☐ Nødvendighed og proportionalitet vurderes (artikel 35, stk. 7, litra b)):
  - ☐ Foranstaltninger, der er planlagt med henblik på overholdelse af forordningen, fastlægges (artikel 35, stk. 7, litra d), og betragtning 90), idet der tages hensyn til:
    - ☐ foranstaltninger, der bidrager til behandlingens proportionalitet og nødvendighed på grundlag af:
      - ☐ udtrykkeligt angivne, legitime formål (artikel 5, stk. 1, litra b))
      - ☐ lovlig behandling (artikel 6)
      - ☐ tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt (artikel 5, stk. 1, litra c))
      - ☐ begrænset opbevaringstid (artikel 5, stk. 1, litra e))
    - ☐ foranstaltninger, der bidrager til de registreredes rettigheder:
      - ☐ oplysninger til den registrerede (artikel, 12, 13 og 14)
      - ☐ indsigtsret og ret til dataportabilitet (artikel 15 og 20)
      - ☐ ret til berigtigelse og til sletning (artikel, 16, 17 og 19)
      - ☐ ret til indsigelse og til begrænsning af behandlingen (artikel 18, 19 og 21)
      - ☐ forbindelser med databehandlere (artikel 28)
      - ☐ garantier i forbindelse med internationale overførsler (kapitel V)
      - ☐ forudgående høring (artikel 36).
- ☐ Risiciene for de registreredes rettigheder og frihedsrettigheder forvaltes (artikel 35, stk. 7, litra (c)):
  - ☐ Oprindelse, karakter, særegenhed og alvor af risiciene vurderes (jf. betragtning 84) eller, mere specifikt, for de enkelte risici (ulovlig adgang, uønskede ændringer og forsvundne data) set fra de registreredes synspunkt:
    - ☐ Der tages hensyn til risikokilder (betragtning 90).
    - ☐ Potentielle virkninger på de registreredes rettigheder og frihedsrettigheder identificeres i tilfælde af begivenheder såsom ulovlig adgang, uønskede ændringer og forsvundne data.
    - ☐ Trusler, der kan føre til ulovlig adgang, uønskede ændringer og forsvundne data, identificeres.
    - ☐ Risikoens sandsynlighed og alvor vurderes (betragtning 90).
  - ☐ Påtænkte foranstaltninger til begrænsning af disse risici fastlægges (artikel 35, stk. 7, litra d), og betragtning 90).
- ☐ Interesserede parter inddrages:
  - ☐ Databeskyttelsesrådgiveren høres (artikel 35, stk. 2).
  - ☐ De registreredes eller deres repræsentanters synspunkter indhentes, hvis det er relevant (artikel 35, stk. 9).