ARTIKKEL 29-ARBEIDSGRUPPEN FOR BESKYTTELSE AV PERSONOPPLYSNINGER

17/00282-1 uoffisiell norsk versjon

WP 248 rev. 01

Retningslinjer for vurdering av personvernkonsekvenser og beslutning om behandlingen kan «medføre en høy risiko» relatert til formålet i 2016/679

Besluttet 4. april 2017

Senest revidert og besluttet 4. oktober 2017

Arbeidsgruppen ble nedsatt i henhold til artikkel 29 i direktiv 95/46/EF. Den er et uavhengig rådgivende EU-organ i spørsmål vedrørende personopplysningsvern og personvern. Dets oppgaver beskrives i artikkel 30 i direktiv 95/46/EF og artikkel 15 i direktiv 2002/58/EF.

Gruppens sekretariat finnes hos direktorat C (Grunnleggende rettigheter og unionsmedborgerskap) i Europakommisjonen, Generaldirektoratet for rettslige spørsmål, B-1049 Brüssel, Belgia, Kontor MO-59 03/075.

Nettsted: http://ec.europa.eu/justice/data-protection/index_en.htm

ARBEIDSGRUPPEN FOR BESKYTTELSE AV PERSONER I FORBINDELSE MED BEHANDLING AV PERSONOPPLYSNINGER,

som er nedsatt ved Europaparlamentets og rådets direktiv 95/46/EF av 24. oktober 1995,

som henviser til artiklene 29 og 30 i dette direktiv,

som henviser til gruppens arbeidsordning

HAR VEDTATT FØLGENDE RETNINGSLINJER:

Innholdsfortegnelse:

Innhold

I. Innledning

Forordning 2016/679[1] (heretter kalt *forordningen*) gjelder fra og med 25. mai 2018. Gjennom artikkel 35 i forordningen innføres begrepet «Vurdering av personvernkonsekvenser» (DPIA)[2], på samme måte som i direktiv 2016/680[3].

En vurdering av personvernkonsekvenser er en prosess som har som formål å beskrive behandlingen, vurdere hvorvidt den er nødvendig og proporsjonal, og bidra til å håndtere de risikoer som behandlingen av personopplysninger medfører for fysiske personers rettigheter og friheter[4], ved å vurdere dem og fastlegge risikoreduserende tiltak. Vurdering av personvernkonsekvenser er viktige verktøy for ansvarlighet, ettersom det ikke bare hjelper den behandlingsansvarlige med å sikre samsvar med kravene i forordningen, men også med å dokumentere at det er gjort tilstrekkelige tiltak for å sikre at forordningen overholdes (se også artikkel 24)[5]. Med andre ord er en **vurdering av personvernkonsekvenser en prosess som skal bidra til å skape og påvise etterlevelse**.

I henhold til forordningen kan manglende overholdelse av krav til vurdering av personvernkonsekvenser medføre at vedkommende tilsynsmyndighet pålegger sanksjoner. Hvis det ikke foretas en vurdering av personvernkonsekvenser der dette er pålagt (artikkel 35 nr. 1 og 35 nr. 3–4), eller hvis den utføres på en uriktig måte (artikkel 35 nr. 2 og 35 nr. 7–9), eller det unnlates å gjøre en forhåndsdrøftelse med vedkommende tilsynsmyndighet når dette er et krav (artikkel 36 nr.3 e), kan dette medføre administrative bøter på opptil 10 millioner euro, eller, om det gjelder en virksomhet, bøter på opptil 2 % av den samlede globale årsomsetningen i forutgående regnskapsår, der det høyeste beløpet anvendes.

---

[1] Europaparlamentets- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EG (generell personvernforordning).

[2]Departementets merknad: I andre land har man skilt mellom PIA (Privacy Impact Assessment) og DPIA (Data Protection Impact Assessment), mens vi i Norge har brukt vurdering av personvernkonsekvenser om begge, mye pga. tidligere versjon av veileder til utredningsinstruksen.

[3] I artikkel 27 i Europaparlamentets- og rådsdirektiv (EU) 2016/680 av 27. april 2016 om vern av fysiske personer i forbindelse med vedkommende myndigheters behandling av personopplysninger med henblikk på å forebygge, etterforske, avsløre eller straffeforfølge straffbare forhold eller iverksette strafferettslige sanksjoner, og om fri utveksling av slike opplysninger fastslås det at det skal gjennomføres en vurdering av personvernkonsekvenser dersom «behandling[en] [...] sannsynlig vil medføre en høy risiko for fysiske personers rettigheter og friheter».

[4] I forordningen blir ikke begrepet "vurdering av personvernkonsekvenser" formelt definert, men

- det spesifiseres i artikkel 35.7 hva vurderingen som minimum skal omfatte i:
    a) en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen, herunder, dersom det er relevant, den berettigede interessen som forfølges av den behandlingsansvarlige,,
    b) en vurdering av om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålene,
    c) en vurdering av risikoene for de registrertes rettigheter og friheter som nevnt i nr. 1, og
    d) de planlagte tiltakene for å håndtere risikoene, herunder garantier, sikkerhetstiltak og mekanismer for å sikre vern av personopplysninger og for å påvise at denne forordning overholdes, idet det tas hensyn til de registrertes og andre berørte personers rettigheter og berettigede interesser.
- mens dens betydning og rolle presiseres i fortalepunkt (84): «For å bedre overholdelsen av denne forordning i tilfeller der det er sannsynlig at behandlingsaktiviteter vil medføre en høy risiko for fysiske personers rettigheter og friheter, bør den behandlingsansvarlige ha ansvar for å foreta en vurdering av personvernkonsekvenser for særlig å vurdere risikoens opprinnelse, art, særegenhet og alvorlighetsgrad».

[5] Se fortalepunkt (84): «Det bør tas hensyn til utfallet av vurderingen ved fastsettelse av egnede tiltak som skal treffes for å påvise at behandlingen av personopplysningene oppfyller kravene i denne forordning».

II. Retningslinjenes anvendelsesområde

I disse retningslinjene tas det hensyn til

- Erklæring 14/EN WP 2186 fra artikkel 29-gruppen vedrørende personvern[6],
- Artikkel 29-gruppens retningslinjer om personvernombud 16/EN WP 243[7],
- Artikkel 29-gruppens uttalelse om formålsbegrensning /EN WP 203[8],
- Internasjonale standarder[9].

I overensstemmelse med den risikobaserte metoden i forordningen er det ikke obligatorisk å utføre en vurdering av personvernkonsekvenser for hver behandling. En vurdering av personvernkonsekvenser kreves kun hvis behandlingen sannsynligvis «*vil medføre en høy risiko for fysiske personers rettigheter og friheter»* (artikkel 35 nr. 1). For å sikre en enhetlig tolkning av de situasjoner hvor en vurdering av personvernkonsekvenser er obligatorisk (artikkel 35 nr. 3), skal disse retningslinjene presisere dette begrepet og gi kriterier for de lister som personvernmyndigheter skal opprette i henhold til artikkel 35 nr. 4.

I henhold til artikkel 70 nr. 1 e kan Det europeiske personvernrådet utstede retningslinjer, anbefalinger og beste praksis for å fremme en enhetlig anvendelse av forordningen. Formålet med dette dokumentet er å forberede fremtidige arbeider fra Det europeiske personvernrådet og klargjøre de aktuelle bestemmelsene i forordningen for å hjelpe behandlingsansvarlige til å følge regelverket, og skape rettssikkerhet for behandlingsansvarlige som er pliktige til å utføre en vurdering av personvernkonsekvenser.

Disse retningslinjene har også som formål å fremme utviklingen av

- en felles EU-liste over behandlingsaktiviteter som omfattes av kravet om vurdering av personvernkonsekvenser (artikkel 35 nr. 4),
- en felles EU-liste over behandlingsaktiviteter som ikke krever en vurdering av personvernkonsekvenser (artikkel 35 nr. 5),
- felles kriterier for metoder som brukes for å utføre en vurdering av personvernkonsekvenser (artikkel 35 nr. 5),
- felles kriterier for å spesifisere når forhåndsdrøftelser skal gjennomføres med tilsynsmyndigheten (artikkel 36 nr. 1),
- anbefalinger som, om mulig, bygger på erfaringer fra EUs medlemsstater.

---

[6] Artikkel 29-gruppens erklæring «*Statement* 14/EN WP 218 *on the role of a risk-based approach in data protection legal frameworks»* (erklæring om en risikobasert metodikk innen den rettslige rammen for beskyttelse av personopplysninger), vedtatt 30. mai 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] Artikkel 29-gruppens retningslinjer om personvernombud 16/EN WP 243, vedtatt 13. desember 2016. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] 8 Artikkel 29-gruppens erklæring 03/2013 om formålsbegrensninger 13/EN WP 203, vedtatt 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, *Risikostyring - Prinsipper og retningslinjer*, Den internasjonale standardiseringsorganisasjonen (ISO), ISO/IEC 29134 (prosjekt), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, Den internasjonale standardiseringsorganisasjonen (ISO).

III. Vurdering av personvernkonsekvenser: forklaringer til forordningen

I henhold til forordningen er behandlingsansvarlig pliktig til å gjennomføre passende tiltak for å sikre og påvise samsvar med forordningen, blant annet når det gjelder «risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter» (artikkel 24 nr.1). De behandlingsansvarliges plikt til i gitte tilfeller å utføre en vurdering av personvernkonsekvenser skal forstås med bakgrunn i deres generelle forpliktelse til å sikre en hensiktsmessig håndtering av de risikoer[10] som oppstår ved behandling av personopplysninger.

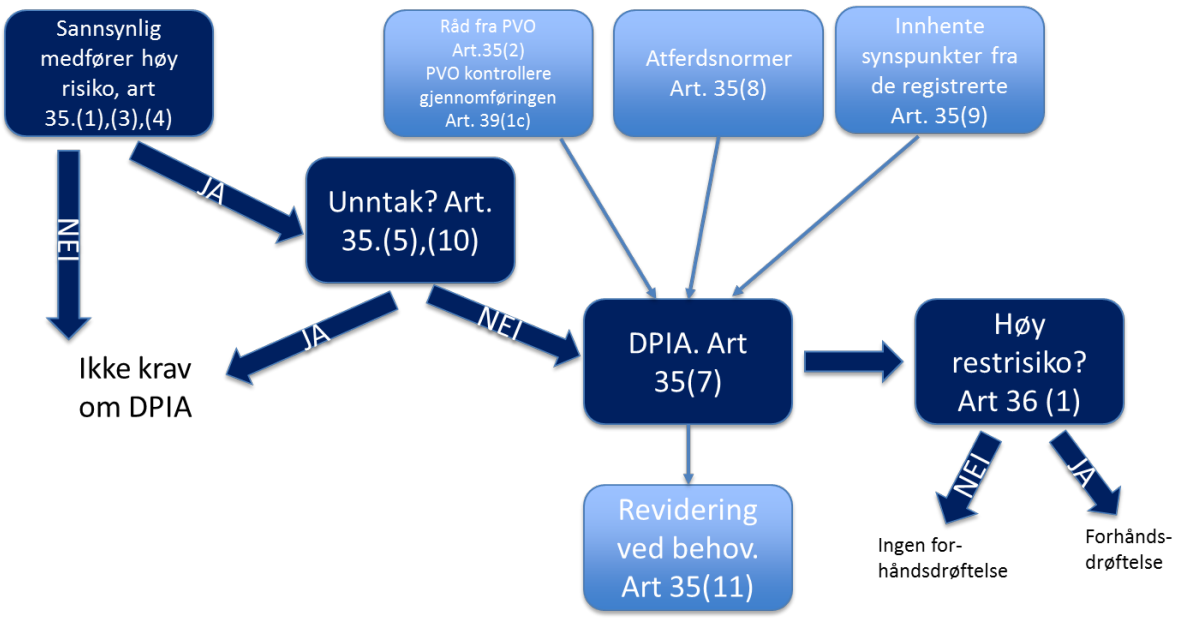
En «risiko» er et scenario som beskriver en hendelse og dens estimerte konsekvenser basert på alvorlighet og sannsynlighet. «Risikohåndtering» kan derimot defineres som samordnede aktiviteter for å styre og kontrollere en virksomhet basert på risiko.

Artikkel 35 viser til sannsynlighet for høy risiko «for fysiske personers rettigheter og friheter». I følge Artikkel 29-gruppens erklæring om betydningen av en risikobasert tilnærming til rettslige rammer for personopplysningsvern, omfatter de registrertes «rettigheter og friheter» først og fremst personopplysningsvern og personvern, men kan også omfatte andre grunnleggende rettigheter så som ytringsfrihet, tankefrihet, bevegelsesfrihet, forbud mot diskriminering, retten til frihet, samvittighets- og religionsfrihet.

I overensstemmelse med den risikobaserte metoden i forordningen er det ikke obligatorisk å utføre en vurdering av personvernkonsekvenser for hver behandling. Det er i stedet kun krav om å utføre en vurdering av personvernkonsekvenser dersom behandlingen sannsynligvis «vil medføre en høy risiko for fysiske personers rettigheter og friheter» (artikkel 35 nr. 1). Selv om vilkårene som utløser plikten til å gjennomføre en vurdering av personvernkonsekvenser ikke er oppfylt, reduseres ikke den behandlingsansvarliges generelle plikter til å gjennomføre tilstrekkelige tiltak for håndtering av risiko relatert til de registrertes rettigheter og friheter. I praksis innebærer dette at behandlingsansvarlige kontinuerlig må vurdere risikoen som oppstår ved deres behandlingsaktiviteter for å identifisere når en type behandling sannsynligvis «vil medføre en høy risiko for fysiske personers rettigheter og friheter».

Følgende figur illustrerer de grunnleggende prinsippene for vurdering av personvernkonsekvenser i forordningen:

[10] Det skal bemerkes at det er en forutsetning ved håndtering av risikoene i forbindelse med fysiske personers rettigheter og friheter, å få identifisert, analysert, estimert, evaluert og behandlet (dvs. redusert) risikoene samt revidert dem regelmessig. Behandlingsansvarlig kan ikke unndra sitt ansvar gjennom å tegne forsikringsavtale på risikoene.



A. Hva skal en vurdering av personvernkonsekvenser håndtere? En enkelt behandling eller et sett av ensartede behandlinger.

En vurdering av personvernkonsekvenser kan omfatte én enkelt behandling av personopplysninger. Det står likevel i artikkel 35 nr. 1 at «*En vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer*». Dessuten står det i fortalepunkt (92) at «*I noen tilfeller kan det være rimelig og økonomisk å utvide vurderingen av personvernkonsekvenser til å omfatte mer enn ett prosjekt, f.eks. dersom offentlige myndigheter eller organer har planer om å innføre en felles applikasjon eller behandlingsplattform, eller dersom flere behandlingsansvarlige planlegger å innføre en felles applikasjon eller et felles behandlingsmiljø på tvers av en industrisektor eller -segment eller for en horisontal aktivitet som er i utstrakt bruk*».

En enkelt vurdering av personvernkonsekvenser kan brukes for å vurdere flere behandlinger som ligner på hverandre med hensyn til karakter, omfang, sammenheng, formål og risiko. Formålet med en vurdering av personvernkonsekvenser er å sikre en systematisk undersøkelse av nye situasjoner som kan medføre høy risiko for fysiske personers rettigheter og friheter, og det ikke er nødvendig å utføre en vurdering av personvernkonsekvenser i situasjoner (dvs. behandlinger som utføres i en spesifikk sammenheng og for et spesifikt formål) som allerede har vært undersøkt. Dette kan være tilfellet når samme type teknologi benyttes til å samle inn samme type opplysninger til samme formål. For eksempel kan en gruppe kommunale myndigheter som hver for seg innfører et lignende kameraovervåkingssystem, utføre én enkelt vurdering av personvernkonsekvenser. Et annet eksempel er et jernbaneselskap (én enkelt behandlingsansvarlig) som gjennomfører én vurdering av personvernkonsekvenser for videoovervåking på samtlige togstasjoner. Dette kan også anvendes ved lignende behandlinger gjennomført av ulike behandlingsansvarlige. I disse tilfellene bør en referanse-vurdering deles eller gjøres offentlig tilgjengelig. Tiltakene som beskrives i vurderingen av personvernkonsekvenser, skal gjennomføres/implementeres og det skal være en begrunnelse for hvorfor én enkelt vurdering er gjennomført.

Om behandlingen omfatter flere behandlingsansvarlige med felles behandlingsansvar, skal deres respektive plikter defineres spesifikt. Vurderingen av personvernkonsekvenser skal vise hvilken av de behandlingsansvarlige som er ansvarlig for de ulike tiltakene som er utformet for å håndtere risiko,

og for å beskytte de registrertes rettigheter og friheter. Hver behandlingsansvarlig bør fremlegge sine behov og dele nyttig informasjon uten å videreformidle konfidensielle opplysninger (f.eks. forretningshemmeligheter, immaterielle rettigheter) eller avsløre sårbarheter.

En vurdering av personvernkonsekvenser kan også være nyttig for å vurdere personvernkonsekvenser av et teknisk produkt, for eksempel maskinvare eller programvare, som sannsynligvis kommer til å bli benyttet av ulike behandlingsansvarlige for ulike behandlinger. Den behandlingsansvarlige som benytter produktet, er naturligvis fremdeles pliktig til å utføre sin egen vurdering av personvernkonsekvenser med hensyn til den konkrete behandlingen, men denne kan understøttes av leverandørens vurdering av personvernkonsekvenser dersom det er relevant. Et eksempel kan være forholdet mellom en produsent av intelligente målere og energileverandører. Den enkelte tilbyder av produktet eller databehandler bør utveksle nyttig informasjon uten å videreformidle forretningshemmeligheter eller skape sikkerhetsrisiko ved å avsløre sårbarheter.

B. Hvilke behandlingsaktiviteter er omfattet av en vurdering av personvernkonsekvenser? Alle behandlingsaktiviteter som sannsynligvis «vil medføre en høy risiko».

I dette avsnittet beskrives de situasjoner hvor en vurdering av personvernkonsekvenser er obligatorisk, og når det ikke er nødvendig å gjennomføre en vurdering av personvernkonsekvenser.

Med mindre behandlingen omfattes av et unntak (III.B.a), skal en vurdering av personvernkonsekvenser utføres når behandlingen sannsynligvis «vil medføre en høy risiko». (III.B.b).

a) Når er det obligatorisk med en vurdering av personvernkonsekvenser? Når behandlingen sannsynligvis «vil medføre en høy risiko».

Forordningen krever ikke at en vurdering av personvernkonsekvenser skal utføres for hver behandling som kan medføre en risiko for fysiske personers rettigheter og friheter. En vurdering av personvernkonsekvenser er bare obligatorisk om behandlingen sannsynligvis «vil medføre en høy risiko for fysiske personers rettigheter og friheter» (artikkel 35 nr. 1, illustrert av artikkel 35 nr. 3 og komplettert av artikkel 35 nr. 4). Det er spesielt relevant når det innføres ny databehandlingsteknologi[11].

I tilfeller der det er usikkert om det er nødvendig å gjennomføre en vurdering av personvernkonsekvenser eller ikke, anbefaler Artikkel 29-gruppen at det gjennomføres en vurdering likevel, fordi det er et nyttig verktøy for behandlingsansvarlig for å overholde personvernforordningen.

Selv om en vurdering av personvernkonsekvenser kan være nødvendig å gjennomføre under andre omstendigheter, er det i artikkel 35 nr. 3 noen eksempler på når en behandling sannsynligvis «vil medføre en høy risiko»:

- «*a) en systematisk og omfattende vurdering av personlige aspekter ved fysiske personer som er basert på automatisert behandling, herunder profilering, og som danner grunnlag for avgjørelser som har rettsvirkning for den fysiske personen eller på lignende måte i betydelig grad påvirker den fysiske personen*[12].

[11] Se fortalepunkt (89), (91) og artikkel 35.1 og 35.3 for flere eksempler.

[12] Se fortalepunkt (75): «særlig for å analysere eller forutsi aspekter som gjelder arbeidsprestasjoner, økonomisk situasjon, helse, personlige preferanser eller interesser, pålitelighet eller atferd, plassering eller bevegelser, for å opprette eller bruke personlige profiler».

- *b) behandling i stor skala av særlige kategorier av opplysninger som nevnt i artikkel 9 nr. 1, eller av personopplysninger om straffedommer og lovovertredelser som nevnt i artikkel 10*[13], eller
- *c) en systematisk overvåking i stor skala av et offentlig tilgjengelig område*.»

Uttrykket «*særlig*» i første setning i artikkel 35 nr. 3 i personvernforordningen viser at dette ikke er ment å være en uttømmende liste. Det kan foreligge «*høy risiko*» ved behandlinger som ikke omfattes av denne listen, men som likevel medfører tilsvarende høy risiko. For slike behandlinger skal det også gjennomføres en vurdering av personvernkonsekvenser. Av denne grunn vil de følgende kriteriene til tider gå lenger enn en ren forklaring av hvordan man skal forstå de tre eksemplene som er gitt i forordningens artikkel 35 nr. 3.

For å gi en mer konkret oversikt over behandlinger som krever en vurdering av personvernkonsekvenser på grunn av behandlingens iboende høye risiko, tatt i betraktning

- de særlige elementene i artikkel 35 nr. 1 og 35 nr. 3 a–c,
- listen som skal besluttes på nasjonalt nivå i samsvar med artikkel 35 nr. 4 og fortalepunkt 71, 75 og 91,
- og andre henvisninger i forordningen for behandlinger som sannsynligvis «*vil medføre en høy risiko*»[14],

skal følgende ni kriterier vurderes:

1. **Evaluering eller poengsetting**, inkludert profilering og forutsigelse, spesielt «*aspekter som gjelder arbeidsprestasjoner, økonomisk situasjon, helse, personlige preferanser eller interesser, pålitelighet eller atferd, plassering eller bevegelser*» (fortalepunkt 71 og (91)). Eksempel på dette kan omfatte finansinstitusjoner som vurderer sine kunder mot en database for kredittopplysning eller mot en database for bekjempelse av hvitvasking og finansiering av terrorisme. Et annet eksempel er et bioteknologiselskap som tilbyr genetiske tester direkte til forbrukere for å vurdere eller forutsi sykdoms-/helserisiko, eller en virksomhet som utvikler atferds- eller markedsføringsprofiler basert på bruken av eller navigeringen på virksomhetens nettside.
2. **Automatiske beslutninger med rettslig eller tilsvarende betydelig virkning**: Behandling som har som formål å ta beslutninger om den registrerte som har «rettsvirkning for den fysiske personen» eller «på lignende måte i betydelig grad påvirker den fysiske personen» (artikkel 35 nr. 3 a). For eksempel kan behandlingen føre til utelukkelse eller forskjellsbehandling av enkeltpersoner. Behandling som har liten eller ingen betydning for enkeltpersoner, oppfyller ikke dette spesielle kriteriet. Ytterlige redegjørelser om disse begrepene vil bli gjort tilgjengelig i de kommende retningslinjene om profilering fra Artikkel 29-gruppen.
3. **Systematisk monitorering**: Behandlingsaktiviteter som brukes for å observere, overvåke eller kontrollere de registrerte, inkludert opplysninger som har blitt samlet inn gjennom nettverk eller «en systematisk overvåking i stor skala av et offentlig tilgjengelig område» (artikkel 35 nr. 3 c)[15]. Denne typen av overvåking/monitorering er et kriterium, siden personopplysninger

[13] Se fortalepunkt (75): «når behandlingen gjelder personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religiøs eller filosofisk overbevisning, fagforeningsmedlemskap, og behandling av genetiske opplysninger, helseopplysninger, seksuelle forhold eller straffedommer og straffbare forhold eller tilknyttede sikkerhetstiltak».
[14] Se f.eks. fortalepunkt (75), (76), (92) og (116).
[15] Artikkel 29-gruppen tolker at «systematisk» innebærer at monitoreringen har ett eller flere av følgende kjennetegn (se Artikkel 29-gruppens retningslinjer om personvernombud 16/EN WP 243):

- monitoreringen skjer etter et system,
- den har vært planlagt i forkant, er organisert eller metodisk,

kan samles inn i situasjoner der de registrerte kanskje ikke er klar over hvem som samler inn opplysningene deres eller hvordan de blir brukt. Dessuten kan det være umulig for enkeltpersoner å unngå å være gjenstand for slik behandling på offentlige områder (eller offentlig tilgjengelig område).

4. **Særlige kategorier av personopplysninger eller opplysninger av svært personlig karakter**: Dette omfatter særlige kategorier av personopplysninger som definert i artikkel 9 (for eksempel informasjon om enkeltpersoners politiske meninger), samt personopplysninger vedrørende straffedommer og lovovertredelser som definert i artikkel 10. Dette gjelder for eksempel et offentlig sykehus som lagrer pasientenes journaler, eller en privatdetektiv som oppbevarer opplysninger om gjerningsmenn. Utover disse bestemmelser i forordningen kan visse kategorier av opplysninger øke den eventuelle risikoen for enkeltpersoners rettigheter og friheter. Slike personopplysninger anses å være fortrolige (som man normalt forstår med dette begrepet), fordi aktivitetene faller inn under privatlivets fred (eks. elektronisk kommunikasjon som skal holdes konfidensiell), eller fordi de påvirker utøvelsen av en grunnleggende rettighet (f. eks. innsamling av sporingsopplysninger som kan reise spørsmål om bevegelsesfrihet) eller krenkelse av disse rettighetene får alvorlige konsekvenser for den registrertes dagligliv (eks. finansielle opplysninger som kan brukes til betalingssvindel). I den forbindelse kan det ha betydning om opplysningene allerede er offentliggjort av den registrerte eller av tredjemann. Det faktum at personopplysningene er offentliggjort, kan anses som et element i vurderingen av om opplysningene forventes brukt videre til spesielle formål. Dette kriteriet kan også omfatte opplysninger som personlige dokumenter, e-post, dagbøker, kommentarer fra lesebrett som er utrustet med kommentarfunksjoner og veldig personlig informasjon i applikasjoner som registrerer aktiviteter.
5. **Personopplysninger behandles i stor skala:** I forordningen defineres ikke hva som menes med stor skala, selv om det gis en viss veiledning i fortalepunkt 91. Artikkel 29-gruppen anbefaler at følgende faktorer vurderes spesielt når man avgjør hvorvidt behandlingen gjennomføres i stor skala[16]:
    a. Antallet registrerte som berøres, enten som et spesifikt antall eller som en andel av den relevante populasjonen.
    b. Mengden og/eller spennvidden i personopplysningene som behandles.
    c. Databehandlingens varighet eller regelmessighet.
    d. Behandlingens geografiske omfang.
6. **Matching eller sammenstilling av datasett** som for eksempel stammer fra to eller flere databehandlingsoperasjoner som gjennomføres med ulike formål og/eller av ulike behandlingsansvarlige på en måte som overstiger den registrertes rimelige forventninger[17].
7. **Personopplysninger om sårbare registrerte (fortalepunkt 75):** Behandling av denne typen av personopplysninger er et kriterium på grunn av den skjeve maktbalansen mellom de registrerte og den behandlingsansvarlige, som betyr at enkeltpersoner kan være ute av stand til, på en enkel måte, å gi sitt samtykke eller motsette seg behandlingen av sine personopplysninger eller utøve sine rettigheter. Sårbare registrerte kan omfatte barn (de kan anses å ikke være i stand til på en bevisst og gjennomtenkt måte å motsette seg eller gi samtykke til behandling av sine personopplysninger), arbeidstakere, mer sårbare

- finner sted som en del i en strategiplan for innsamling av opplysninger,
- og/eller utføres som en del av en strategi.

Artikkel 29-gruppen tolker «offentlig tilgjengelig område» som et sted som er åpent for allmennheten, for eksempel et torg, et kjøpesenter, en gate, et marked, en togstasjon eller et offentlig bibliotek.

[16] Se Artikkel 29-gruppens retningslinjer 16/EN WP 243 om personvernombud.

[17] Se forklaringen i Artikkel 29-gruppens uttalelser 13/EN WP 203 om formålsbegrensninger, s. 24.

befolkningsgrupper som behøver sosial beskyttelse (psykisk syke personer, asylsøkere, eldre personer, pasienter osv.), samt i de situasjoner der det foreligger en ubalanse i forholdet mellom den registrerte og den behandlingsansvarlige.

8. **Innovativ bruk eller anvendelse av ny teknologisk eller organisatorisk løsning**, som en kombinasjon av fingeravtrykk og ansiktsgjenkjenning for en forbedret fysisk adgangskontroll osv. Det går klart frem av forordningen (artikkel 35 nr. 1 og fortalepunkt 89 og 91) at bruk av ny teknologi som defineres «*i samsvar med det oppnådde nivået av teknisk kunnskap*» (fortalepunkt 91), kan medføre behov for å gjennomføre en vurdering av personvernkonsekvenser. Grunnen til dette er at anvendelse av ny teknologi kan medføre nye former for innsamling og bruk av personopplysninger, eventuelt med høy risiko for den enkeltes rettigheter og friheter. De personlige og sosiale konsekvensene ved anvendelsen av ny teknologi kan være ukjente. En vurdering av personvernkonsekvenser hjelper den behandlingsansvarlige å forstå og håndtere slike risikoer. For eksempel kan visse «tingenes internett»-applikasjoner få betydelige konsekvenser for den enkeltes dagligliv og privatliv, og kan derfor kreve en vurdering av personvernkonsekvenser.
9. **Når behandlingen «*hindrer de registrerte i å utøve en rettighet eller gjøre bruk av en tjeneste eller en avtale*»** (artikkel 22 og fortalepunkt 91). Dette omfatter behandlinger som tar sikte på å tillate, endre eller nekte den registrerte tilgang til en tjeneste eller inngå en avtale. For eksempel når en bank kredittvurderer sine kunder mot en database for å avgjøre om de skal tilbys lån.

I de fleste situasjoner kan en behandlingsansvarlig anta at det skal gjennomføres en vurdering av personvernkonsekvenser om to av disse kriteriene er oppfylt. Artikkel 29-gruppen mener generelt at jo flere kriterier behandlingen oppfyller, desto mer sannsynlig er det at det foreligger en høy risiko for de registrertes rettigheter og friheter, og at det derfor er et krav om å gjennomføre en vurdering av personvernkonsekvenser, uavhengig av hvilke tiltak den behandlingsansvarlige har planer om å iverksette.

Likevel kan en behandlingsansvarlig, i gitte tilfeller, vurdere at en behandling som bare oppfyller ett av disse kriteriene, likevel krever en vurdering av personvernkonsekvenser.

Følgende eksempler illustrerer hvordan kriteriene bør anvendes for å vurdere hvorvidt én enkelt behandling krever en vurdering av personvernkonsekvenser:

Eksempler på behandling	**Mulige relevante kriterier**	**Sannsynlig at det er påkrevd å gjennomføre en vurdering av personvernkonsekvenser?**
Et sykehus behandler pasientenes genetiske og pasientdata (sykehusets journalsystem).	• Særlige kategorier av personopplysninger eller opplysninger av meget personlig karakter. • Personopplysninger om sårbare registrerte. • Personopplysninger som inngår i en omfattende behandling.	JA
Bruken av et kamerasystem til å overvåke kjøreatferd på motorveier. Den behandlingsansvarlige tenker å anvende et intelligent videoanalysesystem til å velge ut bestemte biler og gjenkjenne bilskilt automatisk.	• Systematisk monitorering. • Innovativ bruk eller anvendelse av teknologiske eller organisatoriske løsninger.	
En virksomhet overvåker systematisk sine ansattes aktiviteter, herunder deres arbeidsplass, internettaktiviteter osv.	• Systematisk monitorering. • Opplysninger om sårbare registrerte.	
Innsamling av data fra offentlige sosiale medier til generering av profiler.	• Vurdering eller bedømmelse. • Opplysninger som inngår i en omfattende behandling. • Matching eller kombinering av datasett. • Sensitive opplysninger eller opplysninger av svært personlig karakter.	
En institusjon som oppretter en database vedrørende kredittvurdering eller svik på nasjonalt plan.	• Vurdering eller bedømmelse. • Automatisk beslutningstaking med juridisk eller lignende betydelig virkning. • Hindrer registrerte i å utøve en rettighet eller gjøre bruk av en tjeneste eller en avtale. • Sensitive opplysninger eller opplysninger av svært personlig art.	
Lagring med henblikk på arkivering av pseudonymiserte personfølsomme data vedrørende sårbare registrerte i forbindelse med forskningsprosjekter eller kliniske forsøk	• Sensitive opplysninger • Opplysninger om sårbare registrerte. • Hindrer registrerte i å utøve en rettighet eller gjøre bruk av en tjeneste eller en avtale.	
«En leges, helsepersonells eller en advokats behandling av personopplysninger tilhørende pasienter eller klienter» (fortale 91).	• Sensitive opplysninger eller opplysninger av svært personlig karakter. • Opplysninger om sårbare registrerte.	NEI
Et nettmagasin som bruker en e-postliste til å sende en generisk daglig oversikt til abonnentene.	• Opplysninger som inngår i en omfattende behandling.	
En nettbutikk med annonser for deler til veteranbiler som medfører begrenset profilering basert på det	• Vurdering eller bedømmelse.	

som de besøkende har sett på eller kjøpt på nettstedet.		

Omvendt, kan en behandling svare til de situasjoner som er beskrevet ovenfor i tabellen, men den behandlingsansvarlige kan likevel vurdere at behandlingen sannsynligvis ikke «vil medføre en høy risiko». I slike situasjoner bør den behandlingsansvarlige begrunne og dokumentere hvorfor en vurdering av personvernkonsekvenser ikke gjennomføres, og inkludere/notere personvernombudets synspunkter.

Dessuten, som en del av prinsippet om ansvarlighet, skal hver behandlingsansvarlig «*føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar*», inkludert blant annet formålet med behandlingen, en beskrivelse av kategoriene av personopplysningene og mottakere av personopplysningene og «*dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1*» (artikkel 30 nr. 1), og avgjøre hvorvidt en høy risiko er sannsynlig, selv om det til slutt avgjøres at det ikke skal gjennomføres en vurdering av personvernkonsekvenser.

NB: Tilsynsmyndighetene plikter å opprette, offentliggjøre og oversende en liste over de behandlingsaktiviteter som krever en vurdering av personvernkonsekvenser, til Det europeiske personvernrådet (artikkel 35 nr. 4)[18]. De kriteriene som er fastsatt ovenfor, kan hjelpe tilsynsmyndighetene med å opprette en slik liste, som løpende oppdateres med mer spesifikt innehold, hvis relevant. For eksempel kan behandlingen av enhver type biometriske opplysninger eller opplysninger om barn vurderes som relevant i forbindelse med utarbeidelse av en slik liste, artikkel 35 nr. 4.

> b) Når er det ikke et krav om å gjennomføre en vurdering av personvernkonsekvenser? Om behandlingen sannsynligvis ikke «*vil medføre en høy risiko*», eller det foreligger en lignende vurdering av personvernkonsekvenser, eller behandlingen har blitt godkjent før mai 2018, eller har et rettslig grunnlag, eller den er oppført i listen over behandlinger som ikke krever en vurdering av personvernkonsekvenser.

Artikkel 29-gruppen anser at det ikke kreves en vurdering av personvernkonsekvenser i følgende situasjoner:

- Om behandlingen **sannsynligvis ikke «*vil medføre en høy risiko*»** (artikkel 35 nr. 1).
- Om behandlingens art, omfang, sammenheng og formål er veldig **lik en behandling som det har blitt gjennomført en vurdering av personvernkonsekvenser for.** I slike situasjoner kan resultatet fra vurdering av personvernkonsekvenser for lignende behandlinger **brukes** (artikkel 35 nr. 1[19]).
- Om behandlingen **har blitt kontrollert av en tilsynsmyndighet før mai 2018 på særskilte betingelser**, og at disse ikke har endret seg[20] (se III.C).
- Om en behandling **i samsvar med artikkel 6 nr. 1 c eller e,** har et rettsgrunnlag etter EU-retten eller nasjonal lovgiving, der tilhørende lovgivning regulerer den spesifikke

[18] I denne forbindelse «skal vedkommende tilsynsmyndighet anvende konsistensmekanismen nevnt i artikkel 63 dersom slike lister omfatter behandlingsaktiviteter som gjelder tilbud av varer eller tjenester til registrerte eller monitorering av deres atferd i flere medlemsstater, eller som i betydelig grad kan påvirke den frie utveksling av personopplysninger i Unionen» (artikkel 35.6).

[19] «En enkelt vurdering kan omfatte en serie liknende behandlinger som medfører liknende høye risikoer.»

[20] «Beslutninger truffet av Kommisjonen og godkjenninger gitt av tilsynsmyndigheter på grunnlag av direktiv 95/46/EF skal fortsette å gjelde fram til de endres, erstattes eller oppheves.» (Fortalepunkt (171).)

behandlingen og **en vurdering av personvernkonsekvenser allerede er gjennomført** som ledd i utarbeidelse av rettsgrunnlaget (artikkel 35 nr. 10)[21], unntatt hvis medlemsstaten har bestemt at det er nødvendig å gjennomføre en vurdering av personvernkonsekvenser forut for behandlingen.

- Om **behandlingen er på den valgfrie listen (opprettet av tilsynsmyndigheten) over behandlinger** som det ikke kreves vurdering av personvernkonsekvenser for (artikkel 35 nr. 5). En slik liste kan inneholde behandlinger som oppfyller vilkår spesifisert av myndighetene, vanligvis gjennom retningslinjer, spesielle beslutninger eller tillatelser, bestemmelser for etterlevelse osv. (f.eks. i Frankrike, tillatelse, unntak, forenklet regelverk, bestemmelser for etterlevelse osv.). I slike situasjoner, og med forbehold om overprøving av vedkommende tilsynsmyndighet, er det ikke krav om en DPIA. Dette er kun tilfellet dersom behandlingen fullt ut omfattes av de relevante prosedyrene som er angitt i listen, og ellers er fullt ut i samsvar med øvrige relevante krav i forordningen.

C. Hva med allerede igangsatte behandlingsaktiviteter? I visse tilfeller er det påkrevd å gjennomføre vurdering av personvernkonsekvenser.

Kravet om å gjennomføre en vurdering av personvernkonsekvenser gjelder for behandlingsaktiviteter som sannsynligvis medfører høy risiko for fysiske personers rettigheter og friheter, og der det, sett hen til behandlingens art, omfang, sammenheng og formål, har skjedd en endring i risikoen.

Det er ikke et krav om vurdering av personvernkonsekvenser for behandlinger som, i henhold til artikkel 20 i direktiv 95/46/EF, har blitt kontrollert av en tilsynsmyndighet eller personvernombudet, og som gjennomføres på en måte som ikke har endret seg siden den forutgående kontrollen. «*Beslutninger truffet av Kommisjonen og godkjenninger gitt av tilsynsmyndigheter på grunnlag av direktiv 95/46/EF, skal fortsette å gjelde fram til de endres, erstattes eller oppheves.*» (Fortalepunkt 171)

Motsatt innebærer dette at en behandling av personopplysninger som gjennomføres på en måte (omfang, formål, innsamlede personopplysninger, behandlingsansvarliges eller mottakernes identitet, lagringstid, tekniske og organisatoriske tiltak osv.) som har endret seg siden den forutgående kontrollen ble gjennomført av tilsynsmyndigheten eller personvernombudet, og som sannsynligvis vil medføre en høy risiko, bør gjennomgå en vurdering av personvernkonsekvenser.

Dessuten kan det kreves en vurdering av personvernkonsekvenser etter endringer i risikoene som oppstår gjennom behandlingen[22], for eksempel ved at ny teknologi har blitt tatt i bruk eller ved at personopplysninger brukes til et annet formål. Databehandlingsaktiviteter kan utvikle seg raskt og nye sårbarheter kan oppstå. Det bør derfor bemerkes at en revisjon av en vurdering av personvernkonsekvenser ikke bare fremmer kontinuerlige forbedringer, men også er viktig for å opprettholde et høyt beskyttelsesnivå i et miljø som endrer seg over tid. En vurdering av personvernkonsekvenser kan også bli nødvendig på grunn av endringer i behandlingens organisatoriske eller sosiale sammenheng, for eksempel ved at effektene av visse automatiske

[21] Om en vurdering av personvernkonsekvenser gjennomføres ved utarbeidelse av den lovgivning som danner rettsgrunnlag for behandlingen, er en vurdering sannsynligvis påkrevet før behandlingen starter, siden lovgivingen kan avvike fra forslaget på en måte som påvirker privatlivets fred og personopplysningsvern. På det tidspunkt når lovgivingen ble vedtatt, forelå det kanskje ikke heller tilstrekkelige tekniske detaljer om den faktiske behandlingen, selv om det var vedlagt en vurdering av personvernkonsekvenser. I slike tilfeller kan det være nødvendig å gjennomføre en spesifikk vurdering av personvernkonsekvenser før den faktiske behandlingen starter opp.

[22] Avhengig av sammenhengen, innsamlede opplysninger, formål, funksjoner, behandlede personopplysninger, mottakere, kombinasjoner av opplysninger, risiko (underliggende aktiviteter, kilder for risiko, eventuelle påvirkninger, trusler osv.), sikkerhetstiltak og internasjonale overføringer.

beslutninger får økt betydning, eller ved at nye kategorier av registrerte blir sårbare for forskjellsbehandling. Hvert av disse eksemplene kan være et element som medfører endring i risikoen som oppstår ved den aktuelle behandlingen.

Motsatt kan visse endringer også minske risikoen. For eksempel kan en behandling utvikles slik at beslutninger ikke lenger er automatisert, eller at en overvåkningsaktivitet ikke lenger er systematisk. I så fall kan en gjennomført risikoanalyse vise at det ikke lenger er behov for vurdering av personvernkonsekvenser.

God praksis tilsier at **en vurdering av personvernkonsekvenser bør følges opp kontinuerlig og revurderes jevnlig.** Selv om det ikke er et krav om vurdering av personvernkonsekvenser per 25. mai 2018, vil det bli nødvendig for den behandlingsansvarlige å gjennomføre en slik vurdering som ledd i oppfyllelse av de generelle forpliktelsene om ansvarlighet.

D. Hvordan skal vurdering av personvernkonsekvenser gjennomføres?

a) På hvilket tidspunkt skal en vurdering av personvernkonsekvenser gjennomføres? Forut for behandlingen.

Vurdering av personvernkonsekvenser skal gjennomføres «*før behandlingen*» (artikkel 35 nr. 1 og 35 nr. 10, fortalepunkt 90 og 93)[23]. Dette er i samsvar med prinsippene om innebygd personvern og personvern som standardinnstilling (artikkel 25 og fortalepunkt 78). Vurdering av personvernkonsekvenser skal anses som et verktøy til bruk i beslutningsprosesser vedrørende behandlingen.

En vurdering av personvernkonsekvenser bør påbegynnes så tidlig som mulig i utformingen av behandlingsprosessen, selv om enkelte elementer i behandlingsprosessen fremdeles er ukjente. En oppdatering av vurderingen av personvernkonsekvenser under prosjektets livssyklus vil sikre en vurdering av personopplysningsvern og personvern, og vil oppfordre til å utvikle løsninger som fremmer regeletterlevelse. Det kan også være nødvendig å gjenta enkelte steg i vurderingen av personvernkonsekvenser underveis i utviklingsprosessen, siden valg av visse tekniske eller organisatoriske tiltak kan påvirke alvorlighetsgraden eller sannsynligheten for risikoene som kan oppstå gjennom behandlingen.

Det faktum at det kan være behov for en oppdatering av vurderingen av personvernkonsekvenser når behandlingen faktisk er igangsatt, er ikke en gyldig grunn til å utsette eller ikke gjennomføre en vurdering. Vurdering av personvernkonsekvenser er en kontinuerlig prosess, spesielt når behandlingen er dynamisk og endres løpende. **Gjennomføringen av en vurdering av personvernkonsekvenser er en kontinuerlig prosess, ikke en engangsforeteelse.**

b) Hvem er pliktig til å gjennomføre en vurdering av personvernkonsekvenser? Den behandlingsansvarlige, sammen med personvernombudet og databehandleren.

Den behandlingsansvarlige er ansvarlig for å sikre at vurdering av personvernkonsekvenser gjennomføres (artikkel 35 nr. 2). Vurdering av personvernkonsekvenser kan gjennomføres av noen andre, innenfor eller utenfor virksomheten, men den behandlingsansvarlige har det øverste ansvaret for denne oppgaven.

[23] Unntatt om det allerede er en eksisterende behandlingsaktivitet som er kontrollert av tilsynsmyndigheten, i slike tilfeller skal vurderingen av personvernkonsekvenser gjennomføres forut for vesentlige endringer.

Den behandlingsansvarlige må rådføre seg med personvernombudet, dersom det er utpekt et personvernombud (artikkel 35 nr. 2), og disse rådene og de beslutninger som den behandlingsansvarlige tar, bør dokumenteres i vurderingen av personvernkonsekvenser. Personvernombudet skal også kontrollere gjennomføringen av vurderingen av personvernkonsekvenser (artikkel 39 nr. 1 c). Ytterligere veiledning finnes i Artikkel 29-gruppens retningslinjer 16/EN WP 243 om personvernombud.

Om behandlingen helt eller delvis gjennomføres av en databehandler, **bør databehandleren bistå den behandlingsansvarlige i gjennomføringen av vurderingen av personvernkonsekvenser** og fremlegge all nødvendig informasjon (i henhold til artikkel 28 nr. 3 f).

Den behandlingsansvarlige skal «dersom det er relevant, innhente synspunkter på den planlagte behandlingen fra de registrerte eller deres representanter» (artikkel 35 nr. 9). Artikkel 29-gruppen vurderer at:

- Disse synspunktene kan innhentes på ulike måter, avhengig av sammenhengen (f.eks. en generell studie relatert til behandlingsaktivitetens formål og hensikt, et spørsmål til medarbeiderrepresentanter eller vanlige spørreskjema som sendes til den behandlingsansvarliges framtidige kunder), som sikrer at den behandlingsansvarlige har rettslig grunnlag for behandling av personopplysninger som fremkommer ved innhenting av slike synspunkter. Det bør bemerkes at et samtykke til behandling åpenbart ikke er en metode for å få tilbakemeldinger fra de registrerte.
- Om den behandlingsansvarliges endelige beslutninger skiller seg fra de registrertes synspunkter, skal begrunnelsene den behandlingsansvarlige har for å fortsette eller ikke, dokumenteres.
- Den behandlingsansvarlige skal også dokumentere begrunnelsen for ikke å innhente synspunkter fra de registrerte, om han eller hun bestemmer at det ikke er hensiktsmessig, for eksempel om dette kan avsløre forretningssensitiv informasjon, eller vil være uforholdsmessig eller umulig.

Til slutt er det god praksis å definere og dokumentere andre spesifikke roller og ansvarsområder, avhengig av interne strategier, prosesser og regler, for eksempel følgende:

- Når spesifikke avdelinger i virksomheten kan foreslå at det gjennomføres en vurdering av personvernkonsekvenser, bør disse bidra med informasjon til vurderingen, og være involvert i evalueringsprosessen.
- Når det er aktuelt, anbefales det å innhente synspunkter fra uavhengige eksperter fra ulike yrkesgrupper[24] (jurister, IT-eksperter, sikkerhetseksperter, sosiologer, etikkspesialister osv.).
- Databehandleres roller og ansvar skal nedfelles i en avtale. Vurderingen av personvernkonsekvenser skal gjennomføres med hjelp av databehandleren basert på type behandling og den informasjon som er tilgjengelig for databehandleren (artikkel 28 nr. 3 f).
- Den ansvarlige for informasjonssikkerheten, hvis en slik er utpekt, samt personvernombudet, kan foreslå at den behandlingsansvarlige skal gjennomføre en vurdering av personvernkonsekvenser for en bestemt behandling, og bør hjelpe berørte aktører med metodikk, hjelpe til å evaluere kvaliteten på risikovurderingen og hvorvidt restrisikoen er akseptabel, samt utvikle kunnskap som er spesifikk for den behandlingsansvarliges situasjon.
- Den ansvarlige for informasjonssikkerheten, hvis en slik er utpekt, og/eller IT-avdelingen, bør bistå den behandlingsansvarlige og kan foreslå at en vurdering av personvernkonsekvenser skal gjennomføres for en bestemt behandling, avhengig av sikkerhetsbehov eller operative behov.

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

c) Hvilken metode skal benyttes for å gjennomføre en vurdering av personvernkonsekvenser? Ulike metoder, men felles kriterier.

I forordningen fastsettes minimumskriterier for en vurdering av personvernkonsekvenser (artikkel 35 nr. 7 og fortalepunkt 84 og 90):

- *«en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen»,*
- *«en vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene»,*
- *«en vurdering av risikoene for de registrertes rettigheter og friheter»,*
- *«de planlagte tiltakene:*
  - *«for å håndtere risikoene»,*
  - *«for å påvise at denne forordning overholdes»*.

Følgende figur illustrerer den alminnelige, gjentakende prosessen ved gjennomføring av en vurdering av personvernkonsekvenser[25]:

[25] Det må understrekes at den beskrevne prosedyren er gjentakende: I praksis er det sannsynlig at hvert steg gjentas flere ganger innen vurderingen av personvernkonsekvenser kan sluttføres.

Etterlevelse av en atferdsnorm (artikkel 40) må tas i betraktning når personvernkonsekvensene av en behandlingsaktivitet vurderes (artikkel 35 nr. 8). Dette kan være nyttig for å påvise at man har valgt eller iverksatt tilstrekkelige tiltak, forutsatt at atferdsnormen er hensiktsmessig og relevant for behandlingen. Sertifiseringer, segl og merker med den hensikt å påvise at behandlingsansvarliges og databehandleres behandling er i samsvar med forordningen (artikkel 42), samt bindende virksomhetsregler bør også tas i betraktning.

Alle de relevante kravene som foreskrives i forordningen, utgjør en bred, allmenn ramme for utforming og gjennomføring av en vurdering av personvernkonsekvenser. Den praktiske gjennomføringen av en vurdering av personvernkonsekvenser er avhengig av de krav som er fastsatt i forordningen, og som kan kompletteres med mer detaljert praktisk veiledning. Derfor er gjennomføringen av en vurdering av personvernkonsekvenser skalerbar. Dette innebærer at også mindre behandlingsansvarlige kan utforme og gjennomføre en vurdering av personvernkonsekvenser som er tilpasset deres behandlingsaktiviteter.

I forordningens fortalepunkt 90 fastsettes et antall komponenter fra vurdering av personvernkonsekvenser som overlapper med velkjente komponenter for risikohåndtering (f.eks. ISO 31000[26)]. Uttrykt i terminologi fra risikostyring tar en vurdering av personvernkonsekvenser sikte på å «håndtere risikoer» for fysiske personers rettigheter og friheter gjennom å:

- Fastslå sammenheng: «*i det det tas hensyn til behandlingens art, omfang, formål, sammenhengen den utføres i, og kildene til risikoen*»,
- Vurdere risikoene: «*vurdere sannsynligheten for at det vil oppstå høy risiko, samt alvorlighetsgraden av denne*»,
- Håndtere risikoene: «*begrense risikoen*», «*sikre vern av personopplysningene*» og «*påvise at denne forordning overholdes*».

NB: Vurdering av personvernkonsekvenser etter forordningen er et verktøy for å håndtere risikoene for de registrertes rettigheter, og på den måten tar den deres perspektiv, slik tilfellet er innen visse områder (f.eks. samfunnssikkerhet). Motsatt, fokuserer risikostyring på andre områder (f.eks. informasjonssikkerhet) på virksomheten.

Forordningen gir den behandlingsansvarlige en fleksibilitet til å fastsette nøyaktig struktur og form på vurderingen av personvernkonsekvenser, slik at den passer øvrig arbeidsmetodikk og verktøy. Det finnes et antall ulike etablerte prosesser i EU så vel som globalt som tar hensyn til de komponenter som beskrives i fortalepunkt 90. Imidlertid skal en vurdering av personvernkonsekvenser – uansett form – være en unik risikovurdering som gjør det mulig for behandlingsansvarlige å implementere tiltak for å håndtere risikoene.

Ulike metoder (se eksempler på metoder for beskyttelse av personopplysninger og vurdering av personvernkonsekvenser i vedlegg 1) kan benyttes som hjelp i gjennomføringen av de grunnleggende kravene som er fastsatt i forordningen. For å sikre disse ulike fremgangsmåtene, har man identifisert felles kriterier (se vedlegg 2) som hjelper den behandlingsansvarlige med å overholde forordningen. Disse presiserer de grunnleggende kravene i forordningen, men gir tilstrekkelige muligheter for ulike former for gjennomføring. Kriteriene kan benyttes for å påvise at en viss metodikk for vurdering av personvernkonsekvenser oppfyller kravene som stilles i forordningen. **Det er opp til den behandlingsansvarlige å velge metodikk, men metodikken skal være i samsvar med kriteriene som beskrives i vedlegg 2.**

[26] Risikohåndteringsprosesser: kommunikasjon og konsultasjon, etablering av sammenheng, risikovurdering, risikohåndtering, overvåkning og vurdering (se terminologi og definisjoner samt innholdsfortegnelse i ISO 31000-oversikten: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

Artikkel 29-gruppen oppmuntrer til utvikling av sektorspesifikke rammeverk for vurdering av personvernkonsekvenser. Spesifikk bransjekunnskap er nyttig, og medfører at vurderingen av personvernkonsekvenser kan adressere de særegenskaper som foreligger ved en viss type behandling (f.eks. visse typer av opplysninger, forretningsmessige verdier, mulige konsekvenser, trusler, målinger). Dette innebærer at vurderingen av personvernkonsekvenser kan håndtere spørsmål som kommer opp innen bestemte økonomiske sektorer, ved bruk av bestemte teknologier eller ved utførelse av bestemte typer behandlinger.

Til slutt skal «*den behandlingsansvarlige foreta en gjennomgåelse for å vurdere om behandlingen utføres i samsvar med vurderingen av personvernkonsekvenser, i det minste dersom risikoen som behandlingen medfører, endres*.» (Artikkel 35 nr. 11[27]).

d) Er det obligatorisk å offentliggjøre vurdering av personvernkonsekvenser? Nei, men offentliggjøring av et sammendrag kan skape tillit. Den komplette vurderingen av personvernkonsekvenser skal formidles tilsynsmyndigheten ved forhåndsdrøftelse eller på anmodning fra tilsynsmyndigheten.

Offentliggjøring av vurdering av personvernkonsekvenser er ikke et rettslig krav i henhold til forordningen, men en beslutning som den behandlingsansvarlige tar. Behandlingsansvarlig bør imidlertid overveie som minimum å offentliggjøre deler av vurderingen av personvernkonsekvenser, en oppsummering eller konklusjonen av vurderingen.

Formålet med en slik prosess er å bidra til å skape tillit til den behandlingsansvarliges behandlinger, vise ansvar og gjennomsiktighet. Det er spesielt god praksis å offentliggjøre en vurdering av personvernkonsekvenser om behandlingen når offentligheten er berørt. Dette kan særlig være tilfellet dersom det er en offentlig myndighet som gjennomfører en vurdering av personvernkonsekvenser.

Den offentliggjorte vurderingen av personvernkonsekvenser behøver ikke inneholde hele vurderingen, spesielt når den kan inneholde spesifikk informasjon om sikkerhetsrisikoer hos den behandlingsansvarlige eller kompromittere forretningshemmeligheter eller forretningssensitiv informasjon. I slike tilfeller kan den offentliggjorte versjonen være en oppsummering av de viktigste funnene i vurderingen av personvernkonsekvenser, eller til og med bare en uttalelse om at en slik vurdering er gjennomført.

Om en vurdering av personvernkonsekvenser avslører en høy restrisiko, er den behandlingsansvarlige pliktig til å be om en forhåndsdrøftelse med tilsynsmyndigheten før behandlingen igangsettes (artikkel 36 nr. 1). Som ledd i denne prosessen skal hele vurderingen av personvernkonsekvenser fremlegges for tilsynsmyndigheten (artikkel 36 nr. 3.e). Tilsynsmyndigheten kan gi råd[28], og kommer ikke til å avsløre forretningshemmeligheter eller svakheter i sikkerheten, basert på de prinsipper som gjelder i hver medlemsstat om allmenhetens tilgang til offentlige dokumenter.

E. Når skal man gjennomføre forhåndsdrøftelse med tilsynsmyndigheten? Når restrisikoen er høy.

Som forklart ovenfor:

[27] Hvis behandlingen er omfattet av artikkel 35.10, frafaller kun pliktene etter artikkel 35.1–7, men ikke pliktene etter artikkel 35.8,9 og 11.

[28] Det er kun behov for skriftlige råd til den databehandlingsansvarlige når tilsynsmyndigheten anser at den planlagte behandlingen ikke er i overensstemmelse med forordningen jf artikkel 36.2.

- En vurdering av personvernkonsekvenser er påkrevet om en behandling sannsynligvis «vil medføre en høy risiko» (artikkel 35 nr. 1; se III.B.a). Som eksempel kan nevnes at behandling av helseopplysninger i stort omfang sannsynligvis vil medføre en høy risiko og krever en vurdering av personvernkonsekvenser.
- Deretter er det opp til den behandlingsansvarlige å vurdere risikoen for de registrertes rettigheter og friheter og identifisere tiltak[29] som kan redusere disse risikoene til et akseptabelt nivå og påvise samsvar med forordningen (artikkel 35 nr. 7; se III.C.c). Et eksempel kan være anvendelse av tekniske og organisatoriske sikkerhetstiltak ved lagring av personopplysninger på bærbare datamaskiner (effektiv kryptering av hele harddisken, robust nøkkelhåndtering, tilstrekkelig tilgangskontroll, sikrede backup-er osv.), som supplement til eksisterende policy (meddelelse, samtykke, retten til innsyn, retten til innsigelse osv.).

I eksemplet ovenfor med bærbare datamaskiner, kan behandlingen fortsette uten forhåndsdrøftelse med tilsynsmyndigheten i henhold til artikkel 36 nr. 1 og fortalepunkt 84 og 94, om den behandlingsansvarlige mener at risikoene er tilstrekkelig redusert. I tilfeller hvor den behandlingsansvarlige ikke kan håndtere den identifiserte risikoen på en tilfredsstillende måte (dvs. restrisikoen er fremdeles høy), skal den behandlingsansvarlige be om en forhåndsdrøftelse med tilsynsmyndigheten.

Et eksempel på en uakseptabel høy restrisiko er situasjoner der de registrerte kan utsettes for betydelig, eller til og med uopprettelige, konsekvenser som de ikke kan overvinne (f.eks. urettmessig tilgang til opplysninger som innebærer trussel for de registrertes liv, oppsigelse, økonomisk tap), og/eller når det virker innlysende at risikoen vil inntreffe (f.eks. når det ikke er mulig å begrense antall personer som har tilgang til opplysningene på grunn av utvekslings-, anvendelses- eller distribusjonsmetoder, eller om en velkjent sårbarhet ikke kan løses).

Når den behandlingsansvarlige ikke kan finne tilstrekkelige tiltak for å begrense risikoen til et akseptabelt nivå (dvs. restrisikoen er fremdeles høy), er det krav om forhåndsdrøftelse med tilsynsmyndigheten[30].

Dessuten må den behandlingsansvarlige rådføre seg med tilsynsmyndigheten når medlemsstatens nasjonale rett krever at behandlingsansvarlige skal rådføre seg med, og innhente forhåndsgodkjenning fra, tilsynsmyndigheten i forbindelse med en oppgave som utføres av en behandlingsansvarlig i allmennhetens interesse, herunder knyttet til sosial trygghet og folkehelse. (Artikkel 36 nr. 5).

Det må imidlertid presiseres at uansett om det er et krav om forhåndsdrøftelse med tilsynsmyndigheten pga. høy restrisiko eller ikke, så gjelder forpliktelsen om å dokumentere og oppbevare vurderingen av personvernkonsekvenser, og om nødvendig oppdatere den.

IV. Konklusjon og anbefalinger

Vurdering av personvernkonsekvenser er et nyttig verktøy for den behandlingsansvarlige for å sikre at det innføres systemer for behandling av personopplysninger som er i overensstemmelse med forordningen, og kan være obligatoriske for visse typer av behandlinger. De kan tilpasses og kan ha ulik form, men i forordningen fastsettes de grunnleggende kravene for en effektiv vurdering av

[29] Dette skjer med hensyn til de eksisterende retningslinjer fra Det europeiske personvernrådet og tilsynsmyndigheter og med hensyn til det aktuelle tekniske nivået og kostnader for gjennomføringen som foreskrevet i artikkel 35.1.

[30] NB: «pseudonymisering og kryptering av personopplysninger» (samt en minimering av opplysninger, kontrollmekanismer osv.) er ikke nødvendigvis egnede tiltak. De er bare eksempler. Hvilke tiltak som er egnet, er avhengig av sammenhengen og de spesifikke risikoene ved behandlingen.

personvernkonsekvenser. Behandlingsansvarlige må se på gjennomføringen av en vurdering av personvernkonsekvenser som en nyttig og positiv aktivitet som bidrar til etterlevelse av regelverket.

I artikkel 24 nr. 1 fastsettes den behandlingsansvarliges grunnleggende ansvar for etterlevelse av forordningen. «*Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.*»

Vurderingen av personvernkonsekvenser er en grunnleggende del av etterlevelse av forordningen når en behandling av opplysninger med høy risiko planlegges eller pågår. Dette innebærer at behandlingsansvarlige bør anvende de kriteriene som foreskrives i dette dokument for å avgjøre om det må gjennomføres en vurdering av personvernkonsekvenser. Interne strategier for behandlingsansvarlige kan medføre at denne listen utvides utover de rettslige kravene i forordningen. Dette bør resultere i større tillit fra de registrerte og andre behandlingsansvarlige.

Når det planlegges en behandling som sannsynligvis medfører høy risiko, skal den behandlingsansvarlige

- velge en metodikk for å gjennomføre vurdering av personvernkonsekvenser (eksempel gis i vedlegg 1) som oppfyller kriteriene i vedlegg 2, eller spesifisere og gjennomføre en systematisk prosedyre for vurdering av personvernkonsekvenser som
    - er forenlig med kriteriene i vedlegg 2,
    - er integrert i eksisterende revisjonsprosesser vedrørende utforming, utvikling, endring, risiko og operativ kontroll i overenstemmelse med interne prosesser, sammenheng de utføres i og intern kultur,
    - involverer berørte parter og tydelig fastslår deres ansvarsområde (behandlingsansvarlig, personvernombud, registrerte eller deres foresatte, virksomhet, tekniske tjenester, databehandler og ansvarlig for informasjonssikkerhet osv.);
- fremlegge vurderingen av personvernkonsekvenser for vedkommende tilsynsmyndighet, når det foreligger en slik forpliktelse,
- rådføre seg med tilsynsmyndigheten når det ikke lykkes den behandlingsansvarlige å fastsette tilstrekkelige tiltak for å redusere den høye risikoen,
- regelmessig gjennomgå vurderingen av personvernkonsekvenser og de behandlingsaktiviteter som vurderes i denne, og som et minimum når det skjer en endring i risikoen ved behandlingen,
- dokumentere de beslutninger som tas.

Vedlegg 1 – Eksempel på eksisterende rammeverk for vurdering av personvernkonsekvenser i EU

Forordningen spesifiserer ikke bestemte prosedyrer som skal følges ved vurdering av personvernkonsekvenser, men gir i stedet den behandlingsansvarlige handlingsrom til å innføre et rammeverk som kompletterer deres eksisterende rutiner, forutsatt at det inneholder de komponentene som beskrives i artikkel 35 nr. 7. Et slikt rammeverk kan være skreddersydd for den behandlingsansvarlige eller være felles for en bransje. Tidligere offentliggjorte rammeverk som er utviklet av EUs personvernmyndigheter og EU-sektorspesifikke rammeverk, omfatter (men er ikke begrenset til) følgende:

Eksempel på generelle rammeverk innen EU:

- DE: Standard Data Protection Model, V.1.0 – testversion, 2016[31]. https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para una Evaluación de Impacto en 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

Eksempel på sektorspesifikke rammeverk:

Privacy and Data Protection Impact Assessment Framework for RFID Applications[32]. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf

- Data Protection Impact Assessment Template for Smart Grid and Smart metering systems[33]. http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

En internasjonal standard kommer også til å gi veiledning om de metoder som anvendes ved gjennomføring av en vurdering av personvernkonsekvenser (ISO/IEC 29134[34]).

[31] Enstemmig og uttrykkelig godkjent (Bayern unnlot å stemme) ved den 92. konferansen for uavhengige datatilsynsmyndigheter i forbundsstaten og delstatene i Kühlungsborn 9.–10. november 2016.

[32] Se også:

- Kommisjonens anbefaling av 12. mai 2009 om gjennomføring av prinsippene om personvern og personopplysningsvern i forbindelse med anvendelse av radiobølgebasert identifikasjon (RFID). https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Fortale nr. 9/2011 om industriens reviderte forslag til ramme for DPIA i forbindelse med RFID-anvendelse. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_sv.pdf

[33] Se også fortale 7/2013 om modellen for vurdering av personvernkonsekvenser for smarte nett og intelligente målere («DPIA-modellen») utarbeidet av ekspertgruppe 2 i kommisjonens arbeidsgruppe for smarte nettverk. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_sv.pdf

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

Vedlegg 2 – Kriterier for en akseptabel vurdering av personvernkonsekvenser

Artikkel 29-gruppen foreslår følgende kriterier som kan anvendes av de behandlingsansvarlige for å vurdere om en vurdering av personvernkonsekvenser eller en metode for å utføre en vurdering av personvernkonsekvenser er tilfredsstillende for å etterleve forordningen:

- **Det gis en systematisk beskrivelse av behandlingen (artikkel 35 nr. 7 a):**
  - Behandlingens art, omfang, sammenheng og formål tas i betraktning (fortalepunkt 90).
  - Registrering av personopplysninger, mottakere og lagringsperiode.
  - Det gis en funksjonell beskrivelse av behandlingen.
  - De aktiva som er nødvendige for personopplysningene (maskinvare, programvare, nettverk, personer, papir eller forsendelseskanaler for papir), identifiseres.
  - Samsvar med godkjente atferdsnormer tas i betraktning (artikkel 35 nr. 8).

- **Det gjøres en vurdering av nødvendigheten og proporsjonaliteten ved behandlingen (artikkel 35 nr. 7 b):**
  - De planlagte tiltakene for å påvise at forordningen etterleves, fastlegges (artikkel 35 nr. 7 d og fortalepunkt 90), med hensyn til følgende:
  - Tiltak som bidrar til at behandlingen er proporsjonal og nødvendig på grunnlag av
    - Spesifikke, uttrykkelig angitte og berettigede formål (artikkel 5 nr. 1 b),
    - Behandlingens lovlighet (artikkel 6),
    - Adekvat, relevant og begrenset til nødvendige personopplysninger (artikkel 5 nr. 1 c),
    - Begrenset lagringstid (artikkel 5 nr. 1 e).
  - Tiltak som ivaretar de registrertes rettigheter:
    - Informasjon til den registrerte (artiklene 12, 13 og 14).
    - Rett til innsyn og til dataportabilitet (artiklene 15 og 20).
    - Rett til korrigering og sletting (artiklene 16, 17 og 19).
    - Rett til innsigelser og begrensning av behandling (artiklene 18, 19 og 21).
    - Forhold til databehandler (artikkel 28).
    - Tiltak for overføring av personopplysninger til tredjestater eller internasjonale organisasjoner (kapittel V).
    - Forhåndsdrøftelser (artikkel 36).
- **Håndtering av risiko for de registrertes rettigheter og friheter (artikkel 35 nr. 7 c):**
  - Vurdere risikoens opprinnelse, art, særegenhet og alvorlighetsgrad (se fortalepunkt 84) eller, mer spesifikt, for hver risiko (uautorisert tilgang, uautorisert endring og at opplysninger forsvinner), fra de registrertes perspektiv:
    - Risikokilde (fortalepunkt 90).
    - Mulige konsekvenser for de registrertes rettigheter og friheter ved hendelser, herunder uautorisert tilgang, uautorisert endring og tap av opplysninger.
    - Trusler som kan medføre uautorisert tilgang, uautorisert endring og tap av opplysninger.
    - Risikoens sannsynlighet og alvorlighet vurderes (fortalepunkt 90).
  - Beslutte planlagte tiltak for håndtering av risikoene (artikkel 35 nr. 7 d og fortalepunkt 90).
- **Medvirkning fra berørte parter:**
  - Rådføring med personvernombudet (artikkel 35 nr. 2).
  - Synspunkter fra de registrerte eller representanter for registrerte innhentes hvis det er relevant (artikkel 35 nr. 9).