Sjekkliste for vurdering av personvernkonsekvenser (DPIA)

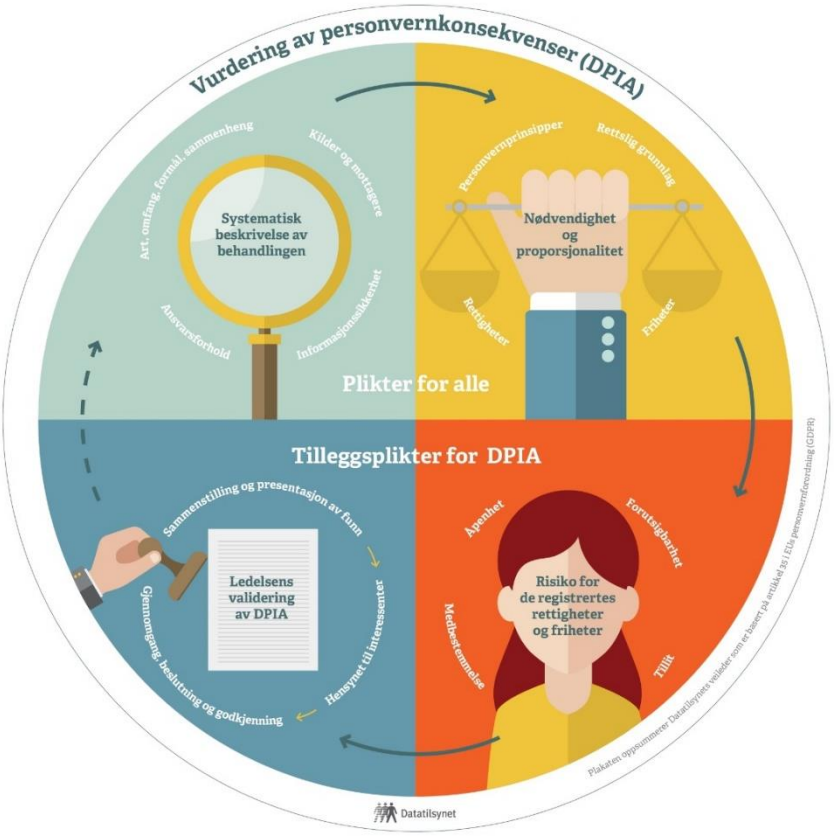
Vi har utarbeidet en sjekkliste med utgangspunkt i kravene i artikkel 35 nr. 7 i personvernforordningen. Det er imidlertid viktig å gå gjennom veilederen vår om vurdering av personvernkonsekvenser *før* dere starter med denne sjekklisten.

Artikkelen sier at vurderingen som et minimum skal inneholde:

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 om de er rimelige i forhold til formålene.
c) En vurdering av risikoene for de registrertes rettigheter og friheter som nevnt i nr. 1 – konsekvenser for personopplysningsvernet.
d) Planlagte tiltak 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.

I tillegg er ansvarlighet et viktig personvernprinsipp, så til slutt må man bedømme og evaluere, og eventuelt godkjenne. I denne fasen har ledelsen eller styret den viktigste rollen. Arbeidet skal sammenstilles og funn presenteres for ledelsen.

Figuren oppsummerer og illustrerer fire faser i den alminnelige, gjentakende prosessen ved gjennomføring av en vurdering av personvernkonsekvenser:



1. En systematisk beskrivelse av behandlingen

Dette kravet forutsetter en gjennomgang av dokumentasjonen dere allerede skal ha i internkontrollen, men der gjennomgangen sees opp mot artiklene 24, 30, 32, 40 og 42. Målet er at den behandlingsansvarlige skal ha en fullstendig oversikt over behandlingen, og sørge for at beskrivelsene som er gjort er komplette og tydelige.

Behandlingens art, omfang, formål og sammenheng

For å få en fullstendig oversikt over behandlingen, må man gå systematisk til verks og sørge for at beskrivelsene er tydelige.

Behandlingens art

Forsikre deg om at beskrivelsen omhandler behandlingens iboende karakteristikk. Dette kan innebære beskrivelser av hva dere planlegger å gjøre med personopplysningene, for eksempel:

- Hvordan skal personopplysningene samles inn? (Samles personopplysningene inn fra den registrerte eller fra andre?)
- Hvordan skal personopplysningene lagres?
- Hvordan skal personopplysningene brukes?
- Hvem skal ha tilgang til personopplysningene?
- Hvem skal det samles inn personopplysninger om? (For eksempel ansatte i egen virksomhet, elever/studenter/barnehagebarn, kunder/klienter/brukere, medlemmer, pasienter, barn)
- Hvordan kan den registrerte utøve sine rettigheter?
- Vil det være en systematisk behandling av personopplysninger?
- Brukes det ny teknologi eller ny bruk av eksisterende teknologi hvor personvernkonsekvenser ikke har blitt vurdert?

Behandlingens omfang

Forsikre deg om at beskrivelsen inkluderer:

- kategorier av personopplysninger (om det behandles personopplysninger som oppleves som private som for eksempel lokasjonsopplysninger, opplysninger om økonomi, kommunikasjon, bekjentskapskrets, og om det behandles særskilte kategorier av personopplysninger som for eksempel opplysninger om helse, rase og religion).
- antall registrerte involvert (i tall eller prosentandel av utvalget).
- volumet av data (antall variabler, detaljeringsgrad).
- frekvensen av behandlingen (om opplysningene innhentes en gang, flere ganger, regelmessig, kontinuerlig, og så videre).
- lagringstiden for personopplysningene (kort, tidsavgrenset, permanent).
- det geografiske omfanget (lokalt, regionalt, nasjonalt, internasjonalt, globalt).

Behandlingens formål

Forsikre deg om at alle formål er beskrevet, det vil si at det er tydelig hva personopplysningene er planlagt å brukes til. Dette omfatter for eksempel:

- Hva er formålet med behandlingen?
- Vil det være kontrollformål (for eksempel skatt, NAV, toll, politi, forsikring)?

- Vil formålet være å treffe avgjørelser om enkeltpersoner basert på systematisk og omfattende analyse av personlige aspekter?
- Vil behandlingen av personopplysninger ha som mål å ta beslutninger som får betydning for den registrerte?
- Skal opplysningene brukes til å profilere den registrerte?
- Brukes personopplysninger for å avdekke ukjente sider eller for å gjenkjenne mønstre ved den registrerte?
- Vil personopplysningene viderebehandles til nye eller andre formål (sekundærbruk som for eksempel forskning)?

Hvilken sammenheng behandlingen utføres i (kontekst)

Dette innebærer å se behandlingen i et større bilde og vurdere alle interne og eksterne faktorer som kan påvirke forventninger eller konsekvenser. Noen eksempler:

- Hvilke kilder brukes for innhenting av personopplysninger?
- Hvilken relasjon har den behandlingsansvarlige med de registrerte? Beskriv maktforholdet mellom den behandlingsansvarlige og de registrerte.
- I hvilken grad har de registrerte kontroll over sine opplysninger?
- Beskriv hvordan behandlingen vil oppfattes fra den registrertes synsvinkel. Kan de registrerte oppfatte behandlingen som uforutsigbar for?
- Vil den registrerte ha en særskilt forventning om konfidensialitet (for eksempel dersom det omhandler helse, velferd, arbeidsforhold, kommunikasjon, lokasjon)?
- Vil den registrerte ha en særskilt forventning om at personopplysningene er nødvendige og korrekte (for eksempel tildeling av velferdsgoder, forsikring, opplysningstjenester)?
- Vil den registrerte ha en særskilt forventning om privatliv (for eksempel i hjemmet og på steder for rekreasjon)?
- Vil det behandles personopplysninger om barn, pasienter eller andre kategorier personer som defineres som sårbare?
- Finnes det tidligere erfaring med tilsvarende type behandling?
- Beskriv eventuelle relevante fremskritt innen teknologi eller sikkerhet.
- Finnes det noen nåværende tilfeller av allmenn bekymring for den beskrevne måten å behandle personopplysninger på?
- Vil dere behandle personopplysninger fra ulike datasett, som er innsamlet for ulike formål og fra ulike behandlingsansvarlige?
- Kobles ulike registre for å gi ny type informasjon om den registrerte? (Kobles for eksempel opplysningene opp mot andre registre eller informasjonssystem.)

Kilder, mottagere, informasjonssikkerhet og ansvarsforhold

Forsikre deg om at oversikten over mottakere, dataflyt og lagring er komplett og tydelig:

- Er alle behandlingsansvarlige, felles behandlingsansvarlige og eventuelle databehandlere identifisert?
- Er alle **mottakere** av personopplysninger identifisert og dokumentert? Gjennomgå det som er relevant av disse punktene:
    - Er alle mottakere/kategorier av mottakere av personopplysningene beskrevet? (ansatte, databehandlere, tredjeparter, eksterne virksomheter og så videre).
    - Hvordan deles personopplysningene mellom avdelinger **internt** i virksomheten? Hvilke personopplysninger deles med hvilke avdeling og hva er formålet med hver av disse delingene? Hvilke **eksterne** virksomheter deles personopplysningene med

(private, offentlige myndigheter og så videre)? Hvilke personopplysninger deles eksternt, for hvilket formål og med hvilke rettslige grunnlag?
    - Overføres personopplysningene til land utenfor EU/EØS-området, og hva er det rettslige grunnlaget for det? Beskriv metode for overføring og land, samt risikovurderingen dere har gjort av landet.
    - Overføres personopplysninger til tredjestater eller internasjonale organisasjoner (artikkel 44-49)?
        - Hvordan sikres etterlevelse av forordningen ved overføring til utlandet?
        - Identifiser andre regelverk, atferdsnormer/bransjenormer og retningslinjer som gjelder ved overføring, og beskriv hvordan disse etterleves.
    - Beskriv hvilke forhåndsregler som tas for å beskytte personopplysninger (taushetserklæringer, databehandleravtale, atferdsnormer/bransjenormer, sikkerhetstiltak og så videre).
    - Har dere en avtale eller kontrakt med eksterne virksomheter om at det er en gjensidig forståelse og ansvar? Gjenspeiler avtalen hvilke begrensninger som gjelder for personopplysningene som deles?
    - Forholdet til databehandlere, gjennomgå:
        - Er alle databehandlerne identifisert og er forholdet til dem avklart gjennom avtaler (artikkel 28 nr. 3)?
            - Er de registrertes rettigheter og friheter ivaretatt i avtalen?
            - Er personvernprinsippene, for eksempel formålsbegrensning, dataminimering, lagring med videre ivaretatt i avtalen?
            - Hvordan sikres informasjonen dere deler hos mottaker? Hva slags opplæring er det for eksempel nødvendig at brukere i eksterne virksomheter får, før de får tilgang til personopplysningene?
    - Gir databehandleren tilstrekkelige garantier for at egnede tekniske og organisatoriske tiltak som sikrer at behandlingen er i samsvar med forordningen (artikkel 28 nr. 1) vil gjennomføres.
- Er all dataflyt, lagring og mellomlagring identifisert?
    - Hvordan overføres og tilgjengeliggjøres personopplysningene (dataflyt)?
    - Hvor og hvor lenge lagres personopplysningene ulike steder?
        - Hvor lenge lagres personopplysningene etter at formålet ved behandlingen er over, før de slettes? Når skal opplysningene slettes? Er det utarbeidet sletterutiner?
    - Dere kan for eksempel bruke dataflytdiagrammer for å illustrere hvilke personopplysninger som skal behandles, hvordan disse beveger seg i/mellom system og eventuelt hvordan de utveksles med andre system.
- Er personopplysningssikkerheten tilstrekkelig ivaretatt? Dette omfatter for eksempel:
    - Er alle iverksatte og planlagte tekniske og organisatoriske tiltak egnet til å sikre personopplysningenes konfidensialitet, integritet og tilgjengelighet? Dette kan for eksempel være sikkerhetsstandarder, policy, adferdsnorm/bransjenorm og så videre.

Gjennomgå den funksjonelle beskrivelsen av alle behandlinger og om alle aktiva som skal brukes er identifisert.

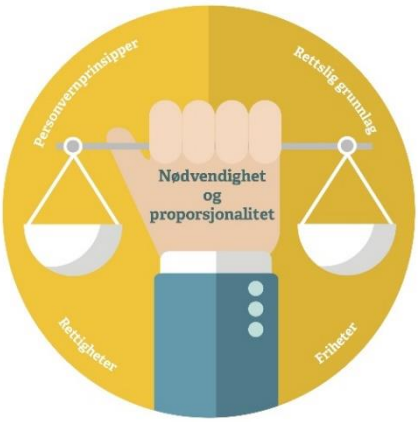
- Gir beskrivelsen et helhetlig og fullstendig bilde av behandlingen? Dette bør omfatte: informasjonssystem, infrastruktur, tjenester, driftsmiljø og ytre grenser, informasjonssystemets tilstøtende grensesnitt med andre systemer og hvordan personopplysningene flyter (overføres mellom ulike systemer).

- Gir beskrivelsen et helhetlig og fullstendig bilde av prosesser og tilknyttede aktiva (maskinvare, programvare, nettverk, personer, papir, kommunikasjonskanaler med videre) som er nødvendige for hele livssyklusen til personopplysninger (fra innsamling til sletting)? For eksempel:
    - Tas ny teknologi i bruk? Eller brukes eksisterende teknologi på en ny måte?
        - Er beskrivelsen tydelig på hvordan dataintegritet, personvern, og sikkerhet er analysert og vurdert når dere valgte denne type teknologi?
    - Har virksomheten bygget systemet fra grunnen av eller er det kjøpt ferdig (som hyllevare) fra en ekstern leverandør og deretter installert hos dere?
    - Er programvaren utviklet med innebygd personvern og personvern som standardinnstilling? Ble det under utvikling tatt valg for å øke personvernet? I tilfelle hvilke?

Forsikre deg om at alle aktuelle referanser som er relatert til og aktuelle for behandlingen er dokumentert. Dette kan omfatte eksterne og interne krav, policy med videre som er nødvendige eller som må etterleves, for eksempel:

- Godkjente atferdsnormer/bransjenormer (artikkel 40).
- Sertifiseringer relatert til personvern (artikkel 42).
- Forskrifter, rundskriv med videre.

2. Nødvendighet og proporsjonalitet



I denne fasen kvalitetssikres det at valgene oppfyller personvernprinsippene, det vil si at de er legitimert og utført for å bidra til at behandlingen er nødvendig. For å etterleve lovkravene, skal dere også sjekke at valgene står i et rimelig forhold til formålene:

Personvernprinsippene

Rettslig grunnlag

Er behandlingen basert på lovlighet, rettferdighet og åpenhet (artikkel 5.1 bokstav a og artikkel 6 og 9)?

- Kommer det rettslige grunnlaget/behandlingsgrunnlaget tydelig frem? For eksempel samtykke, nødvendig for avtale/kontrakt, rettslig forpliktelse, vitale interesser, utøvelse av offentlig myndighet, berettiget interesse.
    - Omfatter rettslig grunnlag både egne formål og utlevering?
- Har dere vurdert og kontrollert behandlingsgrunnlagets gyldighet og rimelighet?
    - Hva er forventede fordeler ved behandlingen? For virksomheten, den registrerte, samfunnet for øvrig og så videre.
    - Skiller dere tydelig mellom hvilke personopplysninger som er om er nødvendig for avtale og hva som skal baseres på samtykke?
- Vurder hvordan åpenhet ivaretas i behandlingen.

Formålsbegrensning

Formål(ene) skal være spesifikt, uttrykkelig angitt og berettiget (artikkel 5.1 bokstav b). Sjekk følgende:

- Er formålet klart definert? Er formålet definert slik at det samsvarer med forventningene til de registrerte?
- Vurder om formålet kan oppnås med en mindre inngripende behandling.
- Vurder hvorvidt formålet kan oppnås med anonyme eller pseudonyme alternativer.

Dataminimering

Personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålene (artikkel 5.1 bokstav c)

- Vurder personopplysningene som skal behandles. Kan formålet oppnås ved for eksempel:
    - å begrense innsamling av personopplysninger?
    - med mindre detaljerte personopplysninger?
    - uten fortrolige eller sensitive personopplysninger?
    - med aggregerte eller pseudonyme opplysninger?
- Begrunn nødvendighet og relevans relatert til formål for hver enkelt variabel i et datasett.

Riktighet

Personopplysninger skal være korrekte og oppdaterte (artikkel 5.1 bokstav d)

- Vurder hvordan personopplysninger holdes korrekte og oppdaterte, med og uten den registrertes involvering.
- Vurder om dere har nødvendig funksjonalitet for å rette og slette uriktige personopplysninger.
- Ut i fra den registrertes perspektiv, er det behov for kontradiksjon? Det vil si den registrertes anledning til å imøtegå det den behandlingsansvarlige har registrert. Et eksempel er en

saksbehandlers beskrivelse av en samtale eller et møte som kan ha elementer av subjektiv oppfattelse av uttalelser, meninger, stemning eller observasjon.
    - Har dere rutiner for hvordan ansatte fører journaler, notater, møtereferat og så videre?

Lagringsbegrensning

Personopplysninger skal slettes eller anonymiseres når formålet er oppnådd (artikkel 5.1 bokstav e).

- Vurder om personopplysninger lagres etter at formålet er oppnådd.
    - Vurder hver enkelt kategori av personopplysninger.
    - Vurder når sletting inntreffer.
    - Vurder eventuelt når personopplysninger anonymiseres eller pseudonymiseres.
- Vurder hvilke garantier som må være plass dersom personopplysninger skal lagres i lenger perioder grunnet arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål (artikkel 89 nr. 1).

Kontroller om det er nødvendig eller mulig å forbedre måten noe av det som er omtalt over er planlagt, avklart eller rettferdiggjort etter personvernregelverket. Der det er mulig, gjennomgå beskrivelsen på nytt eller foreslå ytterligere tiltak for å gi bedre vilkår for de registrerte.

De registrertes rettigheter

Vurder hvordan de registrertes rettigheter ivaretas:

- Vurder hvordan informasjon til de registrerte gis (rettferdig og gjennomsiktig behandling, artikkel 12, 13 og 14).
- Vurder innhenting av samtykke (artikkel 7 og 8).
    - Er det frivillig, uttrykkelig, spesifikt?
    - Dokumenteres samtykke?
    - Kan samtykke trekkes tilbake like enkelt som det gis?
    - Kontroller at samtykke ikke sammenblandes med kontrakt eller personvernerklæring.
- Vurder hvordan den registrertes rett til innsyn og til dataportabilitet ivaretas (artikkel 15 og 20).
- Vurder hvordan den registrertes rett til korrigering og sletting ivaretas (artikkel 16 og 17).
- Vurder hvordan den registrertes rett til innsigelser og begrensning av behandling ivaretas (artikkel 18, 19 og 21).
- Vurder hvordan forbud mot automatiserte individuelle avgjørelser, herunder profilering håndheves (artikkel 22).

Kontroller om det er nødvendig eller mulig å forbedre måten de registrertes rettigheter ivaretas. Der det er mulig, gjennomgå beskrivelsen på nytt eller foreslå ytterligere tiltak.

De registrertes friheter

Vurder hvordan de registrertes friheter i forhold til Den europeiske menneskerettskonvensjonen (EMK) er tatt hensyn til:

- Retten til privatliv og kommunikasjonsvern
- Retten til ikke å bli diskriminert
- Tanke-, tros- og religionsfrihet
- Ytrings-, og informasjonsfrihet

Kontroller om det er nødvendig eller mulig å forbedre måten de registrertes friheter tas hensyn til. Der det er mulig, gjennomgå beskrivelsen på nytt eller foreslå ytterligere tiltak.

3. Vurdering av risiko for de registrertes rettigheter og friheter, og planlagte tiltak for å håndtere risikoene

Gjennom fase 1 har den behandlingsansvarlige kvalitetsjekket at det er en fullstendig oversikt over behandlingen, og at beskrivelsen av den er komplett og tydelig. I fase 2 har behandlingsansvarlig gjennomgått valgene på nytt for å se til at de bidrar til at behandlingen er nødvendig og står i et rimelig forhold til formålene, for å etterleve lovkravene. I denne fasen skal man gjennomføre en vurdering av personvernkonsekvenser for den registrertes rettigheter og friheter.

Medbestemmelse, åpenhet, forutsigbarhet

Gjør en vurdering av risikoens opprinnelse, art, særegenhet og alvorlighetsgrad. Mer spesifikt bør det gjøres en vurdering fra de registrertes perspektiv for hver risiko:

1. **Manglende reell medbestemmelse** - den registrerte har ikke et valg, får ikke informasjon, får ikke innsyn, og så videre.
2. **Manglende reell åpenhet** - virksomheten evner ikke å forklare komplekse behandlinger eller forventet resultat ved sammenstilling av personopplysninger med andre datasett og så videre.
3. **Manglende forutsigbarhet** ved behandlingen - behandlingen er utenfor det den registrerte vil forvente og så videre.

- Avklar potensielle **konsekvenser** for den registrertes personopplysningsvern for hvert risikoscenario. Hvilke konkrete rettigheter og friheter står i fare for å ikke innfris?
    - Rettighetene i artikkel 12-22.
    - Retten til privatliv, kommunikasjonsvern, ytringsfrihet, tanke-, tros- og religionsfrihet, retten til ikke å bli diskriminert og så videre.

  Eksempler på konsekvenser er at den registrerte ikke har mulighet til å utøve sine rettigheter, ikke får tilgang til tjenester eller muligheter, har manglende kontroll over bruken av personopplysninger, utsettes for diskriminering, utsettes for id-tyveri, svindel, økonomiske tap, tap av omdømme, fysisk skade, tap av konfidensialitet, reidentifisering av pseudonymiserte data, eller annen betydelig økonomisk eller sosial ulempe.
- Anslå **alvorlighetsgrad** for hver risiko, særlig avhengig av hvilken inngripen en potensiell virkning har på den registrerte.
- Identifiser **trusler** som kan føre til hendelser og hvilke risikokilder som kan forårsake dem. Hvordan kan dette skje?
- Anslå **sannsynlighet** for at en hendelse oppstår, særlig ut fra en sårbarhetsvurdering og hva slags evne en risikokilde kan ha for å utnytte dem.

Tiltak

Velg tiltak for å håndtere risikoene for de registrertes og andre berørte personers rettigheter og berettigede interesser. Identifiser eller bestem hva slags tiltak (garantier, sikkerhetstiltak og mekanismer) som kan håndtere risikoene. Slike tiltak kan typisk være:

- Spesifikke garantier for å minimere inngripen. For eksempel:
    - krav om fornyet samtykke
    - rett til reservasjon
    - innhenting av registrertes/representanters syn på behandlingen

    - forsterket informasjonsplikt (løpende informasjon, informasjon i flere kanaler, spesifikk informasjon om kobling mellom datasett og resultat av kobling og så videre).
    - særskilt tilrettelagt innsynsportal
    - særskilte dataminimeringstiltak (monitorering bare i bestemte tidsrom eller spesifikke områder, øyeblikksbilder istedenfor kontinuerlig monitorering, avstå fra behandling av spesifikke opplysninger og så videre
    - tilrettelegging for dataportabilitet
    - automatisk sletting eller anonymisering ved kortere intervall enn lovkrav
    - hindre kobling mellom datasett
- Spesifikke sikkerhetstiltak som angår personopplysninger som skal behandles, for eksempel:
    - kryptering
    - anonymisering
    - partisjonering
    - tilgangskontroll
    - sporbarhet
- Generelle sikkerhetstiltak som iverksettes på systemet hvor behandlingen utføres, for eksempel:
    - operativ sikkerhet
    - backup
    - sikkerhet på hardware
    - teknisk og fysisk sikring
- Organisatoriske tiltak (styring), for eksempel:
    - policy
    - rutiner
    - prosjektledelse
    - personellhåndtering og opplæring
    - håndtering av hendelser og brudd
    - forhold til tredjeparter

Kontroller om det er nødvendig eller mulig å forbedre hvert tiltak og beskrivelse etter personvernregelverket og beste praksis innen sikkerhet. Der det er mulig, gjennomgå beskrivelsen på nytt eller foreslå ytterligere tiltak.

Ut fra tiltakene, avgjør om identifiserte risikoer er håndtert og akseptable. Hvis ikke, foreslå ytterligere tiltak og revurder nivået for hver risiko i lys av de nye tiltakene for å fastslå restrisiko.

4. Ledelsens validering av DPIA

Etter at minimumskravene i artikkel 35 nr.7 er gjennomgått, vurdert og beskrevet er det tid for ledelsens validering. Med ordet validere menes i denne sammenhengen å bedømme og evaluere, og eventuelt godkjenne. I denne fasen har ledelsen eller styret den viktigste rollen. Arbeidet skal nå sammenstilles og funn presenteres for ledelsen.

Forutsetninger som ledelsen bør vite om:

- Ledelsen må være bevisst at deres virksomhet behandler personopplysninger som sannsynligvis kan medføre høy risiko for den registrertes rettigheter og friheter, og er omfattet av artikkel 35.
- Ledelsen må få forståelse av den gjennomførte vurderingen av personvernkonsekvenser, identifisert risiko og tiltak.
- Ledelsen må være bevisst at det å ikke gjøre DPIA, utføre DPIA feil, eller ikke rådføre seg med korrekte instanser, kan innebære administrative bøter opptil 10 millioner Euro, eller, om det gjelder en virksomhet, bøter på opptil 2 % av den totale globale årsomsetningen under foregående budsjettår, avhengig av hvilken verdi som er høyest.

Sammenstilling og presentasjon av funn

- Presenter tiltak som er valgt for å sikre at dere overholder de grunnleggende prinsippene for etterlevelse av personvernregelverket (for eksempel: betinget av forbedring eller anses som kompatibel).
- Presenter tiltak som er valgt for å gi tilstrekkelig informasjonssikkerhet i henhold til «beste praksis» (for eksempel: betinget av forbedring eller anses som kompatibel).
- Kartlegg risikoene (opprinnelig eller restrisiko) utifra alvorlighetsgrad og sannsynlighet.
- Utarbeid en handlingsplan basert på tilleggstiltak som ble identifisert under foregående trinn: for hvert tiltak bestem som et minimum hvem som er ansvarlig for gjennomføring, kostnad (økonomisk eller arbeidsbelastning) og estimert tidsramme.

Dokumenter hensynet til interessenter

- Råd og anbefalinger fra personvernombud (artikkel 35 nr. 2).
- Synspunkter fra de registrerte eller deres representanter (artikkel 35 nr. 9).

Ledelsens gjennomgang, beslutning og godkjenning

- Avgjør om hvorvidt de valgte tiltakene, restrisikoen og handlingsplan er akseptabel begrunnet ut fra tidligere identifiserte avveininger og synspunkter fra interessenter.
- Ledelsen beslutter og begrunner om DPIA er
    - Godkjent/validert: Behandling kan starte opp.
    - Betinget av forbedringer (forklar på hvilken måte): Revidert DPIA skal legges frem for ledelsen på nytt.
    - Avvist: Virksomheten beslutter å ikke gjennomføre behandlingen.

Dersom en DPIA har blitt behandlet i ledergruppen mer enn én gang, risikoen fremdeles er høy og viljen til å gjennomføre fremdeles er stor, må dere anmode Datatilsynet om forhåndsdrøftelse. Virksomheten må dokumentere at den ikke greier å gjøre risikoen lavere. Det er ledelsen som tar beslutningen om å anmode Datatilsynet om forhåndsdrøftelse.