**Mal: Vurdering av personvernkonsekvenser (DPIA)**

|  |  |
| --- | --- |
| Navn på system/prosjekt:  |   |
| DPIA-en utføres av:   |   |
| Dato:   |   |

**1. Systematisk beskrivelse av behandlingen**

I denne fasen er målet at den behandlingsansvarlige skal ha en fullstendig oversikt over behandlingen, og sørge for at beskrivelsene som er gjort er komplette og tydelige.

1. Overordnet oversikt

|  |
| --- |
| **Presenter systemet/prosjektet**, og på et overordnet nivå forklar hvilken behandling av personopplysninger den involverer. Her kan man gjerne referere/linke til andre dokumenter, som f.eks. en prosjektskisse. Forklar hvorfor du har identifisert et behov for en DPIA, jf. art. 35 nr. 1.  |

1. **Behandlingens art**

Behandlingens iboende karakteristikk og hvordan behandlingsaktivitetene skal foregå. Beskrivelser av hva dere planlegger å gjøre med personopplysningene.

|  |  |
| --- | --- |
| Hvordan skal personopplysningene samles inn?  | *Samles de f.eks. 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?  | *F.eks. ansatte i egen virksomhet, elever/studenter, pasienter, kunder/klienter osv.*  |
| Hvordan kan den registrerte utøve sine rettigheter?  |   |
| Vil det være systematisk behandling av personopplysninger?  | *Ja/nei*  |
| Brukes det ny teknologi eller ny bruk av eksisterende teknologi hvor personvernkonsekvenser ikke har blitt vurdert?  | *Ja/nei*  |

1. **Behandlingens omfang**

|  |  |
| --- | --- |
| Kategorier av personopplysninger som behandles  | *Behandles særskilte kategorier av personopplysninger eller andre typer personopplysninger som kan oppleves som private?*  |
| Antall registrerte involvert i behandlingen  | *I tall eller evt. prosentandel av et utvalg*  |
| Datavolum  | *Antall variabler, detaljeringsgrad*  |
| Behandlingsfrekvens  | *Hentes opplysningene inn én gang, flere ganger, regelmessig, kontinuerlig osv.*  |
| Lagringstid for personopplysningene  | *Kort, tidsavgrenset, permanent*  |
| Geografisk omfang  | *Lokalt, regionalt, nasjonalt, internasjonalt*  |

1. **Behandlingens formål**

|  |  |
| --- | --- |
| Behandlingens formål  |   |
| Vil det være kontrollformål?  |  |
| Er formålet å treffe avgjørelser om enkeltpersoner basert på systematisk og omfattende analyse av personlige aspekter?  | *Ja/nei*  |
| Har behandlingen av personopplysninger som mål å ta beslutninger som får betydning for den registrerte?  | *Ja/nei*  |
| Skal opplysningene brukes til å profilere den registrerte?  | *Ja/nei*  |
| Brukes personopplysninger for å avdekke ukjente sider eller for å gjenkjenne mønstre ved den registrerte?  | *Ja/nei*  |
| Vil personopplysningene viderebehandles til nye eller andre formål?  | *Sekundærbruk som f.eks. forskning. Ja/nei*  |

1. **Sammenhengen behandlingen utføres i (kontekst)**

Her er målet å se behandlingen i et større bilde og vurdere alle interne og eksterne faktorer som kan påvirke forventninger eller konsekvenser.

|  |  |
| --- | --- |
| Hvilke kilder brukes for innhenting av personopplysninger?  |   |
| Relasjon mellom behandlingsansvarlig og den registrerte   | *Beskriv maktforholdet*  |
| I hvilken grad har den registrerte kontroll over sine opplysninger?  |   |
| Beskriv hvordan behandlingen vil oppfattes fra den registrertes synsvinkel  | *Kan de registrerte oppfatte behandlingen som uforutsigbar?*  |
| Vil den registrerte ha en særskilt forventning om konfidensialitet?  | *F.eks. dersom det omhandler helse, arbeidsforhold, kommunikasjon, lokasjon osv.*  |
| Vil den registrerte ha en særskilt forventning om at personopplysningene er nødvendige og korrekte?  | *F.eks. tildeling av velferdsgoder, opplysningstjenester.*  |
| Vil den registrerte ha en særskilt forventning om privatliv?  | *F.eks. i hjemmet og på steder for rekreasjon.*  |
| Vil det behandles personopplysninger om barn, pasienter eller andre kategorier av personer som defineres som sårbare?  |   |
| Finnes det tidligere erfaring med tilsvarende type behandling?  |   |
| Beskriv eventuelle relevante fremskritt innen teknologi eller sikkerhet  | *Dersom dette er relevant*  |
| 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 f.eks. opplysningene opp mot andre registrerte eller informasjonssystemer?*  |

1. **Identifisering og oversikt**

|  |  |
| --- | --- |
| Behandlingsansvarlig:  |   |
| Felles behandlingsansvarlig:  | *Hvis relevant*  |
| Databehandler(e):   | *Hvis relevant*  |

1. **Mottakere av personopplysninger**

|  |  |
| --- | --- |
| Beskriv alle mottakere/kategorier av mottakere av personopplysninger  | *F.eks. ansatte, databehandlere, tredjeparter, eksterne virksomheter osv.*  |
| Hvordan deles personopplysningene mellom avdelinger **internt** i virksomheten?  | *Hvilke opplysninger deles med hvilke avdelinger, og hva er formålet med hver av delingene?*  |
| Hvilke **eksterne** virksomheter deles personopplysningene med? Hvis ja, for hvilke formål og med hvilke rettslige grunnlag?  | *Private bedrifter, offentlige myndigheter osv.*  |
| Overføres personopplysningene til land utenfor EU/EØS-området (tredjestater), jf. art. 44-49? Hvis ja, hva er det rettslige grunnlaget for det?  | *Forklar hvordan dere sikrer etterlevelse av forordningen ved overføring til utlandet. Identifiser eventuelle andre regelverk, atferdsnormer/bransjenormer og retningslinjer som gjelder ved overføring, og beskriv hvordan disse etterleves.*  |
| Beskriv hvilke forholdsregler som tas for å beskytte personopplysninger  | *F.eks. taushetserklæringer, databehandleravtale, sikkerhetstiltak osv.*  |
| Er alle databehandlere identifisert, og er forholdet til dem avklart gjennom avtaler, jf. art. 28 nr. 3?  | *Er de registrertes rettigheter og friheter ivaretatt i avtalen? Er personvernprinsippene ivaretatt i avtalen? Hvordan sikres informasjonen dere deler hos mottaker?*  |
| Gir databehandleren tilstrekkelige garantier for at egnede tekniske og organisatoriske tiltak som sikrer at behandlingen er i samsvar med forordningen, vil gjennomføres?  |   |

1. **Dataflyt, lagring og mellomlagring**

|  |  |
| --- | --- |
| 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?   |   |
| Er personopplysningssikkerheten tilstrekkelig ivaretatt?  | *Er f.eks. alle iverksatte og planlagte tekniske og organisatoriske tiltak egnet til å sikre personopplysningenes konfidensialitet, integritet og tilgjengelighet? Kan f.eks. være sikkerhetsstandarder, policy, atferdsnorm/bransjenorm osv.*  |

1. **Informasjonssikkerhet**

|  |  |
| --- | --- |
| Gjennomgå den funksjonelle beskrivelsen av alle behandlinger og om alle aktiva som skal brukes er identifisert  | *Bør omfatte informasjonssystem, infrastruktur, tjenester, driftsmiljø, ytre grenser, informasjonssystemets tilstøtende grensesnitt med andre systemer og hvordan personopplysningene flyter (overføres mellom ulike systemer)*  |
| Tas ny teknologi i bruk, eller brukes eksisterende teknologi på en ny måte?  |   |
| Har virksomheten bygget systemet fra grunnen av eller er det kjøpt ferdig (som hyllevare)) fra ekstern leverandør og deretter installert hos dere?  |   |
| Er programvaren utviklet med innebygd personvern og personvern som standardinnstilling?  |   |

Forsikre deg om at alle aktuelle referanser som er relatert til og aktuelle for behandlingen er dokumentert. Kan omfatte eksterne og interne krav, policy mv. som er nødvendige eller som må etterleves, f.eks.:

* Godkjente atferdsnormer/bransjenormer (art. 40)
* Sertifiseringer relatert til personvern (art. 42)
* Forskrifter, rundskriv, mv.

**2. Nødvendighet og proporsjonalitet**

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

2.1 Personvernprinsippene

2.1.1 Rettslig grunnlag

|  |  |
| --- | --- |
| Rettslig grunnlag/behandlingsgrunnlag:  |   |
| Kommer det rettslige grunnlaget/behandlingsgrunnlaget tydelig frem for de registrerte?   |   |
| Omfatter rettslig grunnlag både egne formål og eventuell utlevering?  |   |
| Vurder hvordan åpenhet ivaretas i behandlingen  |   |

2.1.2 Formålsbegrensning

Formål(ene) skal være spesifikt, uttrykkelig angitt og berettiget, jf. art. 5 nr. 1 bokstav b.

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

2.1.3 Dataminimering

Personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålene, jf. art. 5 nr. 1 bokstav c.

|  |  |
| --- | --- |
| Vurder om formålet kan oppnås med mindre datainnhenting  | *F.eks. begrense innsamling av personopplysninger, mindre detaljerte personopplysninger, uten fortrolige/sensitive personopplysninger etc.*  |
| Begrunn nødvendighet og relevans relatert til formål for hver enkelt variabel i et datasett  |   |

2.1.4 Riktighet

Personopplysninger skal være korrekte og oppdaterte, jf. art. 5 nr. 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 opplysninger  |   |
| Ut ifra den registrertes perspektiv, er det behov for kontradiksjon?  | *Dvs. den registrertes anledning til å imøtegå det den behandlingsansvarlige har registrert, f.eks. en saksbehandlers beskrivelse av en samtale.*  |

2.1.5 Lagringsbegrensning

Personopplysninger skal slettes eller anonymiseres når formålet er oppnådd, jf. art. 5 nr. 1 bokstav e.

|  |  |
| --- | --- |
| Vurder om personopplysninger lagres etter at formålet er oppnådd  | *Vurder hver enkelt kategori av personopplysninger, når sletting inntreffer, og evt. når personopplysninger anonymiseres eller pseudonymiseres.*  |
| Vurder hvilke garantier som må være på plass dersom personopplysninger skal lagres i lenge perioder grunnet arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål, jf. art. 89 nr. 1.  |   |

2.2 De registrertes rettigheter

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

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

I denne fasen skal man gjennomføre en vurdering av personvernkonsekvenser for den registrertes friheter og rettigheter etter forordningen. Først litt generelt om hva som skal gjøres her, så følger malen under.

3.1 Medbestemmelse, åpenhet og forutsigbarhet

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

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

Her skal man også avklare potensielle **konsekvenser** for den registrertes personopplysningsvern for hvert risikoscenario. Hvilke konkrete rettigheter og friheter står i fare for å ikke innfris?

Eksempler på konsekvenser: Den registrerte har ikke mulighet til å utøve sine rettigheter, får ikke 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, 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.
* Anslå **sannsynlighet** for at en hendelse oppstår, særlig ut fra en sårbarhetsvurdering og hva slags evne en risikokilde kan ha for å utnytte dem.

3.2 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:
* 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 osv.)
* Særskilt tilrettelagt innsynsportal
* Særskilte dataminimeringstiltak (monitorering bare i bestemte tidsrom eller spesifikke områder, øyeblikksbilder i stedet for kontinuerlig monitorering, avstå fra behandling av spesifikke opplysninger osv.)
* Tilrettelegging for dataportabilitet
* Automatisk sletting eller anonymisering ved kortere intervall enn lovkrav
* Hindre kobling mellom datasett
* Spesifikke sikkerhetstiltak som angår personopplysninger som skal behandles:
* Kryptering
* Anonymisering
* Partisjonering
* Tilgangskontroll
* Sporbarhet
* Generelle sikkerhetstiltak som iverksettes på systemet hvor behandlingen utføres:
* Operativ sikkerhet
* Back-up
* Sikkerhet på hardware
* Teknisk og fysisk styring
* Organisatoriske tiltak:
* Policy
* Rutiner
* Prosjektledelse
* Personellhåndtering og opplæring
* Håndtering av hendelser og brudd
* Forhold til tredjeparter

Identifiser og vurder risikoer:

|  |  |  |  |
| --- | --- | --- | --- |
| **Beskriv risikoen behandlingen har for de registrertes rettigheter og friheter, og hvilke konsekvenser den har for de registrerte**  | **Alvorlighetsgrad for risikoen**  | **Identifiser trusler som kan føre til hendelser**  | **Sannsynlighet for at en hendelse oppstår**  |
|   | *Minimal, betydelig, alvorlig*  |   | *Liten, mulig, høy*  |

Identifiser risikoreduserende og skadebegrensende tiltak:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risiko**  | **Tiltak**  | **Effekt** **på** **risiko**  | **Restrisiko**  | **Tiltak** **godkjent**  |
|   |   | *Eliminert, redusert eller akseptert*  |   | *Ja/nei*  |

**4. Ledelsens validering av personvernkonsekvensvurderingen (DPIA)**

|  |  |  |
| --- | --- | --- |
| **Moment**  | **Navn og dato**  | **Kommentarer**  |
| Tiltak godkjent av:  |   |   |
| Restrisiko godkjent av:  |   | *Dersom restrisiko med høy risikograd blir godkjent, ta kontakt med Datatilsynet før oppstart for forhåndsdrøfting, jf. art. 36 nr. 1.*  |
| Personvernombudsbistand gitt:  |   | *Personvernombudet skal gi råd om regelverksoverholdelse, steg 6-tiltak og om hvorvidt behandlingsaktiviteter kan settes i gang, jf. art. 35 nr. 2 og art. 39 nr. 1 bokstav c.*  |
| Sammendrag av personvernombudets råd:         |
| Personvernombudets råd er akseptert eller overprøvd av:  |   | *Hvis overprøvd, må du forklare bakgrunnen for dette*  |
| Kommentarer:  |
| De registrertes synspunkter er innhentet og gjennomgått av:   |   | *Hvis din avgjørelse avviker fra de registrertes synspunkter, bør du forklare bakgrunnen for at du velger å sette i gang/fortsette behandlingen*  |
| Kommentarer:  |
| Denne personvernkonsekvensvurderingen vil følges opp av:   |   | *Personvernombudet bør også følge opp personvernkonsekvensvurderingen løpende, jf. art. 39 nr. 1 bokstav c.*  |