**Mal for**

**Data Protection Impact Assessment (DPIA) –**

**Personvernkonsekvensutredning etter GDPR**

Denne malen er utviklet på bakgrunn av krav i GDPR. Det er tatt hensyn til Datatilsynets veiledning om DPIA. En del av teksten er hentet fra Datatilsynets sjekkliste for vurdering av personvernkonsekvenser. Malen gir et bilde av momentene som **bør** vurderes i en DPIA. Den enkelte virksomhet som bruker malen må selv konkret vurdere innhold og omfang av egen DPIA. Tabellene i malen er ikke uttømmende og må tilpasses de enkelte behandlingene som omfattes av en DPIA.

|  |
| --- |
| **DEL I. Vurdering av behov for DPIA** |

[I denne delen er det kun nødvendig å besvare spørsmålene i tabellen nedenfor, ingen analyse.]

Når må DPIA gjennomføres?

*«Dersom det er sannsynlig at en* ***type behandling****, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens* ***art, omfang, formål og sammenhengen den utføres i****, vil medføre en* ***høy risiko*** *for fysiske personers* ***rettigheter og friheter****, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for vernet av personopplysninger.»* (GDPR art.35.1)

Kriterier når DPIA *kan* bli et krav:

1. **Evaluering eller scoring**, spesielt knyttet til arbeidsresultater, økonomisk situasjon, helse, personlige preferanser eller interesser, oppførsel og adferd, lokasjon og bevegelser osv.
2. **Automatiserte beslutninger** med juridisk eller tilsvarende betydning.
3. **Systematisk overvåking** av registrerte.
4. **Særlige kategorier personopplysninger** eller **andre sensitive personopplysninger av høy personlig karakter** (sistnevnte spesielt knyttet de enkeltes «friheter», men kan også omfatte f.eks. økonomiske og finansielle opplysninger).
5. **Databehandling i stort omfang**, som at det er et stort antall registrerte involvert, store mengder data, mange ulike typer data, lang varighet av behandlingen, stor geografisk utbredelse av behandlingen osv.
6. **Kombinering eller sammenstilling av datasett**.
7. Personopplysninger vedrørende **spesielt sårbare registrerte** (som barn, ansatte, psykisk syke, asylsøkere, eldre, pasienter mv.).
8. **Innovativ eller nyskapende bruk av personopplysninger,** som f.eks. bruk av biometriske data for tilgangskontroll, Internet of Things-løsninger, velferdsteknologi osv.
9. Når behandlingen i seg selv **forhindrer eller begrenser de registrertes mulighet til å utøve sine rettigheter** etter loven eller avtale, eller **bruke tjenester**.

Vurderingsspørsmål om behov for DPIA:

| Nr. | Vurderingsspørsmål | Ja/Nei |
| --- | --- | --- |
| 1. | Er dette et nytt prosjekt eller prosess? |  |
| 2. | Vil prosjektet innebære innsamling av ny informasjon om enkeltpersoner? |  |
| 3. | Vil prosjektet be enkeltpersoner om å gi informasjon om seg selv? |  |
| 4. | Vil informasjon om enkeltpersoner bli delt med organisasjoner eller personer som ikke tidligere har hatt rutinemessig tilgang til informasjonen? |  |
| 5. | Skal du bruke informasjon om enkeltpersoner som er innsamlet for et formål, men der opplysningene for tiden ikke er eller ikke lenger er i bruk (ikke behandles utover lagring)? |  |
| 6. | Innebærer prosjektet at du bruker ny teknologi som kan oppfattes som inngripende for personvernet? For eksempel, bruk av biometri eller ansiktsgjenkjenning? |  |
| 7. | Vil prosjektet resultere i at du tar beslutninger eller gjennomfører tiltak mot enkeltpersoner på måter som kan ha en betydelig innvirkning på dem? |  |
| 8. | Basert på typen informasjon om enkeltpersoner, er det spesielt sannsynlig at bekymringen for eller forventninger til personvernet vil øke? |  |
| 9. | Vil prosjektet kreve at du kontakter personer på måter som de kan finne inngripende? |  |

Dersom svaret er "ja" på ett eller flere av spørsmålene ovenfor, kan det bety at det er behov for DPIA. Forsett til DEL II.

|  |
| --- |
| **DEL II. Grunnleggende utgangspunkter og beskrivelser** |

**II.1. Bakgrunn**

* Forutsetninger og avgrensning
* Hvem som deltar i DPIA (DPIA-team)
* Interessenter

**II.2. Løsning, tjeneste og system**

* Beskrivelse av løsning, tjeneste og system (eller konsept)

Beskrivelsen bør omfatte: informasjonssystem, infrastruktur, tjenester, driftsmiljø og ytre grenser, informasjonssystemets tilstøtende grensesnitt med andre systemer og hvordan personopplysningene flyter (overføres mellom ulike systemer).

* Beskrivelse av behandling av personopplysninger i løsning, tjeneste og system (inkl. informasjonsflyt)

Beskrivelsen bør omfatte 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).

**II.3. Behandlingens omfang**

* Beskrivelse av alle opplysninger som behandles
  + hvilke typer opplysninger (særlige kategorier eller ikke)
* Kategorier av de registrerte (for eksempel barn, foreldre, pasienter, ansatte osv.)
* Volumet av data (antall variabler, detaljeringsgrad).
* Frekvensen av behandlingen (om opplysningene innhentes en gang, flere ganger, regelmessig, kontinuerlig, og så videre).
* Det geografiske omfanget (lokalt, regionalt, nasjonalt, internasjonalt, globalt).

**II.4. Formålsbeskrivelser**

* Beskrivelse av formålet med behandlingen av personopplysninger

[Det må presiseres:

* + Formålet med hele løsningen
  + Formålet med behandling av personopplysninger i løsningen generelt
  + Formålet med detaljerte typer av behandlingsaktiviteter dersom de har ulike formål]

| Nr. | Vurderingsspørsmål | Svar (forklar svar) |
| --- | --- | --- |
| 1. | Hva er formålet med behandlingen? |  |
| 2. | Vil formålet være å treffe avgjørelser om enkeltpersoner basert på systematisk og omfattende analyse av personlige aspekter? |  |
| 3. | Vil behandlingen av personopplysninger ha som mål å ta beslutninger som får betydning for den registrerte? |  |
| 4. | Skal opplysningene brukes til å profilere den registrerte? |  |
| 5. | Brukes personopplysninger for å avdekke ukjente sider eller for å gjenkjenne mønstre ved den registrerte? |  |

|  |
| --- |
| **DEL III. Behandlingens lovlighet** |

**III.1. Hjemmelsgrunnlag**

| Nr. | Vurderingsspørsmål | Svar (forklar svar) |
| --- | --- | --- |
| 1. | Finnes det hjemmelsgrunnlag i forskrift eller lov for behandlingen av personopplysninger? |  |
| 2. | Finnes det annet rettsgrunnlag for behandlingen (for eksempel samtykke, avtale, verne vitale interesser, utførelse av myndighetsoppgave, oppfylle rettslig forpliktelse, jf. GDPR art.6)? |  |
| 3. | Finnes det konsesjon eller forhåndsgodkjenning fra REK eller Datatilsynet, eller dispensasjon fra taushetsplikten? |  |

* Gjennomgang av rettsgrunnlag, konsesjoner og dispensasjoner.
* Gjennomgang av begrensninger eller mulighetsrom som rettsgrunnlag, konsesjoner eller dispensasjoner gir.

**III.2. Samtykke**

| Nr. | Vurderingsspørsmål | Svar (forklar svar) |
| --- | --- | --- |
| 1. | Forutsettes det samtykke for behandlingen? |  |
| 2. | Hvordan vil samtykke bli innhentet? |  |
| 3. | Er alle kravene til samtykke oppfylt? Samtykke fra den registrerte må være frivillig, spesifikk, informert og utvetydig (GDPR art.4). |  |
| 4. | Dokumenteres samtykke? |  |
| 5. | Kan samtykke trekkes tilbake like enkelt som det gis? |  |
| 6. | Foreligger det informasjon til den registrerte om muligheten til å trekke tilbake samtykke? |  |
| 7. | Omfatter samtykket alle behandlinger og behandlingsformål som nevnt i DEL IV? |  |

* Gjennomgang av samtykke og vilkår for samtykke. Kontroller at samtykke ikke sammenblandes med kontrakt eller personvernerklæring.
* Gjennomgang av begrensninger eller mulighetsrom som samtykket gir. Beskriv hvordan den registrertes rettigheter ivaretas i vilkårene for samtykke.

**III.3. Viderebehandling**

[Dette punktet besvares kun dersom behandlingen er en viderebehandling av personopplysninger som tidligere er samlet inn for et formål.]

| Nr. | Vurderingsspørsmål | Svar (forklar svar) |
| --- | --- | --- |
| 1. | Behandles opplysninger videre til andre formål enn opprinnelig formål (for eksempel forskning)? | Hvis ja, beskriv viderebehandlingene og hvilke opplysninger som viderebehandles. |
| 2. | Dersom rettsgrunnlag for opprinnelig behandling av personopplysninger er lov eller forskrift, åpner lov eller forskrift for viderebehandling av personopplysninger? |  |
| 3. | Dersom opprinnelig behandling er basert på samtykke, dekker samtykket viderebehandlingen av de samme personopplysningene? | Hvis svaret er nei, vil det innhentes nytt samtykke? |
| 4. | Viderebehandles personopplysninger for statistiske formål? | Hvis ja, finnes det nødvendige garantier for å ivareta personvernet? Nevn garantier. |

**III.4. Vurdering av formålet sett opp mot rettsgrunnlag**

| Nr. | Vurderingsspørsmål | Svar (forklar svar) |
| --- | --- | --- |
| 1. | Er formålet eller formålene klart definert? |  |
| 2. | Er formålet nedfelt i forskrift eller lov? |  |
| 3. | Vil det være kontrollformål (for eksempel i annen lovgivning innenfor skatt, NAV, toll, politi, forsikring?) |  |
| 4. | Er det noe i egen forskrift eller andre forskrifter eller lover som begrenser formålet? |  |
| 5. | Er formålet beskrevet i løsning, tjeneste eller system utfordrende sett opp mot rettsgrunnlaget? |  |
| 6. | Omfatter rettslig grunnlag både egne formål og utlevering? |  |
| 7. | Er formålet definert slik at det samsvarer med forventningene de registrerte kan ha ut fra egen forskrift, lov eller samtykkevilkår? |  |

**III.5. Oppsummering**

Her oppsummeres kort vurderingene som er gjort i DEL III.

|  |
| --- |
| **DEL IV. Behandling av personopplysninger** |

**IV.1. Oversikt over behandling og behandlingsaktiviteter**

| Nr. | Behandling | Detaljert beskrivelse av behandlingsaktiviteter |
| --- | --- | --- |
| 1. | Innsamling |  |
| 2. | Lagring |  |
| 3. | Deling |  |
| 4. | Gi tilgang til |  |
| 5. | Retting |  |
| 6. | Sletting |  |

**IV.2. Systematisk beskrivelse og vurdering av behandling av personopplysninger**

## **IV.2.1. Innsamling**

| Nr. | Vurderingsspørsmål | Svar (forklar svar) |
| --- | --- | --- |
| 1. | Hvilke typer personopplysninger samles inn? |  |
| 2. | Er noen av personopplysningene over kategorisert som særlige kategorier av personopplysninger? (for eksempel helseopplysninger, rase, fagforening osv.) |  |
| 3. | Hvordan samles personopplysningene inn? |  |
| 4. | Samles personopplysningene inn direkte fra de registrerte selv eller fra andre kilder? | Nevn evt. datakilder det samles opplysninger fra. |
| 5. | Er det noe som er særlig inngripende ved måten personopplysningene samles inn (for eksempel ved hjelp av fingeravtrykk, kamera- eller lydopptak, eller sporing av en persons lokasjon, biometri)? |  |
| 6. | Samles det inn flere opplysninger enn det som er nødvendig ut fra formålet? |  |
| 7. | Får den registrerte all informasjon som er påkrevd etter GDPR art.13 og 14? |  |

## **IV.2.2. Lagring**

| Nr. | Vurderingsspørsmål | Svar (forklar svar) |
| --- | --- | --- |
| 1. | Hvordan skal opplysningene lagres? |  |
| 2. | Hvor og hvor lenge lagres personopplysningene? | Vurder hver enkelt type personopplysninger og ulike lagringssteder |
| 3. | Hvilke kriterier brukes for å bestemme lagringstid? | Vurder hver enkelt type personopplysninger |
| 4. | Når skal personopplysningene slettes? |  |
| 5. | Etter at formålet ved behandlingen er oppnådd, hvor lenge lagres personopplysningene før de slettes? |  |
| 6. | Er det utarbeidet rutiner for sletting? |  |
| 7. | Gis det informasjon til den registrerte om muligheten til å slette opplysninger og hvordan sletting kan gjøres? |  |

## **IV.2.3. Deling**

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Vurderingsspørsmål | | Svar (forklar svar) |
| 1. | Utleveres eller tilgjengeliggjøres det personopplysninger til andre utenfor virksomheten? | |  |
| 2. | Hvordan utleveres eller tilgjengeliggjøres personopplysningene (dataflyt)? | | Illustrer hvordan personopplysningene beveger seg i /mellom systemer og eventuelt hvordan de utveksles med andre systemer. |
| 3. | Er alle mottakere av personopplysninger identifisert og dokumentert (for eksempel ansatte, databehandlere, tredjeparter, eksterne virksomheter osv.)? | |  |
| 4. | a. | Hvordan deles personopplysningene mellom avdelinger internt i virksomheten? |  |
| b. | Hvilke personopplysninger deles med hvilke avdelinger og hva er formålet med hver av disse delingene? |  |
| 5. | a. | Hvilke eksterne virksomheter deles personopplysningene med (private, offentlige myndigheter osv)? |  |
| b. | Hvilke personopplysninger deles eksternt, for hvilket formål og med hvilke rettslige grunnlag? |  |
| 6. | Vil personopplysningene overføres til andre land utenfor EU/EØS-området, og hva er det rettslige grunnlaget for overføringen? | | Hvis ja, beskriv metode for overføring og land, samt risikovurderingen som er gjort. |
| 7. | Vil personopplysninger overføres til tredjestater eller internasjonale organisasjoner (GDPR art.44-49)? | |  |
| 8. | Hvordan sikres etterlevelse av forordningen ved overføring til utlandet? | |  |
| 9 | Finnes det annet regelverk, atferdsnormer/bransjenormer og retningslinjer som må følges? | |  |

## **IV.2.4. Tilgang**

|  |  |  |
| --- | --- | --- |
| Nr. | Vurderingsspørsmål | Svar (forklar svar) |
| 1. | Hvem har tilgang til opplysninger? |  |
| 2. | Finnes det dokumentert rutiner for tilgangsstyring? |  |
| 3. | Vil tilgangsstyringen for brukergruppene være rollebasert og tidsbegrenset? |  |
| 4. | Dersom det gis tilgang utenfor virksomheten, er det signert databehandleravtaler eller taushetserklæring? |  |

## **IV.2.5. Retting**

|  |  |  |
| --- | --- | --- |
| Nr. | Vurderingsspørsmål | Svar (forklar svar) |
| 1. | Finnes det mulighet for retting av feil i den registrertes opplysninger? |  |
| 2. | Gis det informasjon til den registrerte om muligheten til å rette opplysninger og om hvordan retting kan gjøres? |  |
| 3. | Finnes det dokumenterte rutiner for retting? |  |
| 4. | Dersom den registrerte ikke selv kan rette feil i egne personopplysninger, finnes det andre måter å gjøre det på? |  |

## **IV.2.6. Sletting**

|  |  |  |
| --- | --- | --- |
| Nr. | Vurderingsspørsmål | Svar (forklar svar) |
| 1. | Finnes det mulighet for sletting av den registrertes opplysninger? |  |
| 2. | Gis det informasjon til den registrerte om muligheten til å slette opplysninger og om hvordan sletting kan gjøres? |  |
| 3. | Finnes det dokumenterte rutiner for sletting? |  |
| 4. | Dersom den registrerte ikke selv kan slette egne personopplysninger, finnes det andre måter å gjøre det på? |  |
| 5. | Finnes det rettsgrunnlag i lov eller forskrift som gir grunnlag for å nekte sletting? | Hvis ja, henvis til hjemmelen. |

**IV.3. Vurdering av sammenheng behandlingen utføres i (kontekst)**

[I denne delen vurderes behandlingen i et større bilde. Alle interne og eksterne faktorer som kan påvirke forventninger eller konsekvenser vurderes her.]

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Vurderingsspørsmål | | Svar (forklar svar) |
|  | Vil det behandles personopplysninger fra ulike datasett, som er innsamlet for ulike formål og fra ulike behandlingsansvarlige? | |  |
|  | Hvilke kilder brukes for innhenting av personopplysninger? | |  |
|  | a. | Kobles systemene der opplysninger behandles opp mot andre informasjonssystemer? | Hvis ja, beskriv formålet med koblingen og hvordan koblingen gjøres |
| b. | Finnes det tidligere erfaring med tilsvarende type behandling? |  |
|  | Finnes det noen nåværende tilfeller av allmenn bekymring for den beskrevne måten å behandle personopplysninger på? | |  |
|  | Hvilken relasjon har den behandlingsansvarlige med de registrerte? Beskriv maktforholdet mellom dem. | |  |
|  | Med tanke på at kompleksitet i den sammenheng behandlingen utføres i (kontekst), i hvilken grad har de registrerte kontroll over sine opplysninger? | |  |
|  | Beskriv hvordan behandlingen vil oppfattes fra den registrertes synsvinkel. Kan for eksempel de registrerte oppfatte behandlingen som lite forutsigbar? | |  |
|  | Vil den registrerte ha en særskilt forventning om konfidensialitet (for eksempel dersom det omhandler helse, velferd, arbeidsforhold, kommunikasjon, lokasjon)? | |  |

**IV.4. Innebygd personvern**

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Vurderingsspørsmål | | Svar (forklar svar) |
|  | Hvordan tenkes innebygd personvern og personvern som standardinnstilling ivaretatt i løsningen med tanke på: | | |
| a. | kravene til design? |  |
| b | sikker koding? |  |
| c. | testing og godkjenning før produksjonssetting? |  |
| d. | kontinuitets- og beredskapsplaner? |  |
| e. | jevnlige revisjoner? |  |
| f. | opplæring? |  |
|  | Er alle prinsippene for behandling av personopplysninger ivaretatt i løsningen? – Se DEL V.1 | |  |
|  | Hvordan er den registrertes rettigheter ivaretatt i løsningen? – Se DEL V.2 for hvilke rettigheter er det snakk om. | |  |
|  | Tas ny teknologi i bruk? | | Hvis ja, beskriv på hvordan dataintegritet, personvern, og sikkerhet er analysert og vurdert ved valg denne type teknologi – Se DEL VI.1.1. og VI.1.2. |
|  | Brukes eksisterende teknologi på en ny måte? | | Hvis ja, beskriv på hvordan dataintegritet, personvern, og sikkerhet er analysert og vurdert ved valg denne nye måten – Se DEL VI.1.1. og VI.1.2. |

**IV.5. Ansvarsforhold**

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Vurderingsspørsmål | | Svar (forklar svar) |
|  | a. | Er det noen avtale eller kontrakt med eksterne virksomheter om gjensidig forståelse for ansvar og roller? |  |
| b. | Gjenspeiler avtalen hvilke begrensninger som gjelder for behandling av personopplysningene? |  |
| 2. | a. | Brukes det databehandler? |  |
| b. | Er alle databehandlerne identifisert og er forholdet til dem avklart gjennom avtaler (GDPR art.28 nr.3)? |  |
| 3. | Om databehandleravtale: | | |
| a. | Gir databehandleren tilstrekkelige garantier for at egnede tekniske og organisatoriske tiltak som sikrer at behandlingen er i samsvar med forordningen (GDPR art.28 nr.1) vil gjennomføres? |  |
| b. | Er personvernprinsippene, for eksempel formålsbegrensning, dataminimering, lagring med videre ivaretatt i avtalen? |  |
| c. | Er de registrertes rettigheter og friheter ivaretatt i avtalen? |  |

**IV.6. Vurdering av behandlingene samlet**

|  |  |  |
| --- | --- | --- |
| Nr. | Vurderingsspørsmål | Svar (forklar svar) |
| 1. | Vil planlagte behandlinger gjøre det lett eller vanskelig for den registrerte å utøve sine rettigheter? |  |
| 2. | Vil planlagte behandlinger ut fra den registrertes synsvinkel preges av uforutsigbarhet eller lite åpenhet? |  |
| 3. | Er det usikkerhet knyttet til hvordan grunnleggende prinsipper for behandling av personopplysninger ivaretas (GDPR art.5)? |  |

**IV.7. Oppsummering**

Her oppsummeres kort vurderingene som er gjort i DEL IV.

|  |
| --- |
| **Del V. Nødvendighet og forholdsmessighet av behandlingen** |

[Denne delen inneholder en vurdering av om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålene med behandlingen.]

**V.1. Personvernprinsippene**

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Vurderingsspørsmål | | Svar (forklar svar) |
| 1 | Er behandlingen basert på lovlighet, rettferdighet og åpenhet (GDPR art.5.1 bokstav a og art.6 og 9)? | |  |
| a. | Kommer det rettslige grunnlaget/behandlingsgrunnlaget tydelig frem? |  |
| b. | Vurder rimeligheten av behandlingen: Hva er forventede fordeler ved behandlingen? For virksomheten, den registrerte, samfunnet for øvrig osv. |  |
| c. | Hva vil konsekvensene være dersom behandlingene ikke gjennomføres? |  |
| d. | Vurder hvordan åpenhet ivaretas i behandlingen. |  |
| 2 | Formålsbegrensninger | | |
| a. | Er formålet definert slik at det samsvarer med forventningene til de registrerte? |  |
| B | Har det vært vurdert andre alternativer for å oppnå formålet med behandlingen? | Hvis ja, beskriv |
| c. | Finnes det mindre personverninngripende alternativer for å oppnå det samme formålet? | Hvis ja, beskriv. |
| D | Vurder hvorvidt formålet kan oppnås med anonyme eller pseudonyme alternativer. |  |
| 3 | Dataminimering.  Kan formålet oppnås ved for eksempel: | | |
| a. | å begrense innsamling av personopplysninger? |  |
| b. | med mindre detaljerte personopplysninger? |  |
| c. | uten fortrolige eller sensitive personopplysninger? |  |
| Begrunn nødvendighet og relevans relatert til formål for alle opplysninger som behandles. | |  |
| 4 | Riktighet | | |
| a. | Vurder hvordan personopplysninger holdes korrekte og oppdaterte, med og uten den registrertes involvering. |  |
| b. | Vurder om det finnes nødvendig funksjonalitet for å rette og slette uriktige personopplysninger, ref. punkt IV.2.5 og IV.2.6. | Hvis ja, beskriv |
| c. | Har dere rutiner som ivaretar kravet til korrekte og oppdaterte personopplysninger? | Hvis ja, beskriv. |
| 5 | Lagringsbegrensning | | |
| a. | Vurder om personopplysninger lagres etter at formålet er oppnådd og når opplysningene slettes. |  |
| b. | Vurder når personopplysninger anonymiseres eller pseudonymiseres som muliggjør videre lagring. |  |
| c. | 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 (GDPR art.89 nr.1). |  |
| 6. | Integritet og konfidensialitet – se DEL VI.1. | | |

**V.2. Ivaretakelse av de registrertes rettigheter**

|  |  |  |
| --- | --- | --- |
| Nr. | Vurderingstemaer | Vurdering |
| 1. | Vurder hvordan informasjon til de registrerte gis (prinsippet om rettferdighet og åpenhet i behandlingen) (GDPR art.12, 13 og 14). |  |
| 2. | Vurder hvordan den registrertes rett til innsyn ivaretas (GDPR art.15). |  |
| 3. | Vurder hvordan den registrertes rett til retting og sletting ivaretas (GDPR art.16 og 17). |  |
| 4. | Vurder hvordan den registrertes rett til innsigelser og begrensning av behandling ivaretas (GDPR art.18, 19 og 21). |  |
| 5. | Vurder hvordan den registrertes rett til dataportabilitet ivaretas (GDPR art.20). |  |
| 6. | Vurder hvordan forbud mot automatiserte individuelle avgjørelser, herunder profilering håndheves (GDPR art.22). |  |

**V.3. Ivaretakelse av de registrertes friheter**

|  |  |  |
| --- | --- | --- |
| Nr. | Vurderingstemaer | Svar (forklar svar) |
| 1. | 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 |  |

**V.4. Oppsummering**

Her oppsummeres kort vurderingene som er gjort i DEL V.

|  |
| --- |
| **Del VI. Personvern risikoanalyse og planlagte tiltak** |

[Denne delen inneholder vurdering av risiko for de registrertes rettigheter og friheter, samt planlagte tiltak for å håndtere risikoene].

**VI.1. Risiko, konsekvenser og sannsynlighet**

## **VI.1.1. Sikkerhet ved behandlingen**

[Fokuset i denne delen bør være sikkerhet i løsningen]

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Vurderingsspørsmål | | Svar (forklar svar) |
|  | Er personopplysningssikkerheten tilstrekkelig ivaretatt? | |  |
| a. | Er det gjort en risikovurdering av løsningen (også ved endringer)?  Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet. |  |
| b. | Er det gjennomført tiltak for å håndtere risiko?  Ved valg av tiltak skal det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter. |  |
| c. | Er restrisiko håndterbar og akseptabel? |  |
| 2. | Er alle iverksatte og planlagte tekniske og organisatoriske tiltak egnet til å sikre personopplysningenes konfidensialitet, integritet og tilgjengelighet? | |  |
| 3. | Beskriv hvilke forhåndsregler som tas for å beskytte personopplysninger (taushetserklæringer, databehandleravtale, atferdsnormer/bransjenormer, sikkerhetstiltak osv). | |  |

## **VI.1.2 Personopplysningsvernet**

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Vurderingstemaer | | Vurdering |
| 1. | Med utgangspunkt i den registrertes perspektiv for hver risiko kan for eksempel følgende vurderes: | | |
| a. | Manglende reell medbestemmelse - den registrerte har ikke et valg, får ikke informasjon, får ikke innsyn, og så videre. |  |
| b. | Manglende reell åpenhet - virksomheten evner ikke å forklare komplekse behandlinger eller forventet resultat ved sammenstilling av personopplysninger med andre datasett og så videre |  |
| c. | Manglende forutsigbarhet ved behandlingen - behandlingen er utenfor det den registrerte vil forvente og så videre. |  |
| 2. | Hvilke konkrete rettigheter og friheter står i fare for å ikke innfris, jf. GDPR art.12-22 (rettigheter) og retten til privatliv, kommunikasjonsvern, ytringsfrihet, tanke-, tros- og religionsfrihet, retten til ikke å bli diskriminert og så videre (friheter)? | |  |

Generelt for vurdering av "Sikkerhet ved behandlingen" og "Personopplysningsvernet":

* Vurder risikoens opprinnelse, art, særegenhet og alvorlighetsgrad.
* Avklar potensielle **konsekvenser** for den registrertes personopplysningsvern for hvert risikoscenario.
* Anslå **alvorlighetsgrad** for hver risiko, særlig avhengig av hvilken inngripen en potensiell virkning har på den registrerte.
* Identifiser **trusler** og egenskaper ved løsningen 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.

**VI.2. Vurdering av planlagte tiltak**

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Vurderingstemaer | | Vurdering |
| 1. | Beskriv tiltak for å håndtere risikoene for de registrertes og andre berørte personers rettigheter og berettigede interesser.  Eksempler på tiltak kan være:   * Garantier: krav til fornyet samtykke, rett til reservasjon osv. * Sikkerhetstiltak: tilgangskontroll, anonymisering, kryptering osv. * Mekanismer: funksjonalitet som er personvernfremmende for eksempel logging og sperring av tilgang eller sperring av informasjon | | Presiser hva slags tiltak (garantier, sikkerhetstiltak og mekanismer) |
| 2. | Ut fra tiltakene, vurder om: | | |
| a. | sikringen av vernet av personopplysninger er tilstrekkelig | Beskriv hvordan. |
| b. | de registrertes og andre berørte personers rettigheter og berettigede interesser er hensyntatt | Beskriv hvordan. |
| c. | identifiserte risikoer er håndtert og akseptable |  |
| d. | det er restrisiko etter alle planlagte tiltak |  |

Kontroller om det er nødvendig eller mulig å forbedre hvert tiltak etter personvernregelverket og beste praksis innen sikkerhet. Hvis ikke, foreslå ytterligere tiltak og revurder nivået for hver risiko i lys av de nye tiltakene for å fastslå restrisiko.

**VI.3. Oppsummering**

Her oppsummeres kort vurderingene som er gjort i DEL VI.

|  |
| --- |
| **Del VII. Involvering av personvernombudet** |

[I denne delen legges det opp til en vurdering fra personvernombudet. Personvernombudet involveres etter at DEL I – VI av denne malen er gjennomført.]

|  |
| --- |
| Vurdering fra personvernombudet |
|  |

|  |
| --- |
| **Del VIII. Ledelsens godkjenning og forhåndsdrøftelse med Datatilsynet** |

[I denne delen legges opp til en validering av DPIA av ledelsens gjennomgang, beslutning og godkjenning.]

|  |  |  |
| --- | --- | --- |
| Nr. | Vurderingstemaer | Vurdering |
| 1. | Ledelsen vurderer hvorvidt de planlagte tiltakene, restrisikoen og handlingsplan er akseptable. |  |
| 2. | 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 ikke å 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 i tråd med GDPR art.36. Virksomheten må dokumentere at den ikke greier å gjøre risikoen lavere. Det er ledelsen som tar beslutningen om å anmode Datatilsynet om forhåndsdrøftelse.

\*\*\*\*\*

Lenke til Datatilsynets sjekkliste: <https://www.datatilsynet.no/globalassets/global/regelverk/veiledere/dpia-veileder/sjekkliste-for-dpiafaser.pdf>

Lenke til uoffisiell norsk versjon av retningslinjer for vurdering av personvernkonsekvenser og beslutning om behandlingen kan "medføre en høy risiko" fra Artikkel 29-Arbeidsgruppen for beskyttelse av personopplysninger:

<https://www.regjeringen.no/contentassets/1b6b0aebf624465f9704cadeaa320269/veileder_vurdering_personvernkonsekvenser_norsk_versjon.pdf>

© 2018. Direktoratet for e-helse. Malen er utviklet av GDPR-prosjektet i Direktoratet for e-helse, og tilpasset egne forhold i direktoratet. Alle virksomheter er selv ansvarlige for å vurdere om innhold i malen er dekkende for egne behov. Merk at direktoratet jobber kontinuerlig med å oppdatere malen for internt bruk, og anbefaler alle virksomheter som bruker malen til å gjøre vurderinger av når det er nødvendig med egne oppdateringer.

Etter GDPR art.83.4 bokstav a kan manglende eller feil utførelse av DPIA, eller manglende rådføring med korrekte instanser, innebære administrative bøter for Behandlingsansvarlig 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.