Vurdering av personvernkonsekvenser (DPIA) for innføring av nytt fagsystem

Vurdering gjennomført dd.mm.åå

Innholdsfortegnelse

[Informasjon om gjennomføringen av DPIA 3](#_Toc182842099)

[Innledende vurdering 4](#_Toc182842100)

[Systematisk beskrivelse av behandlingen 5](#_Toc182842101)

[Beskrivelse av fagsystemet som behandlingen skal utføres i 5](#_Toc182842102)

[Beskrivelse av behandlingens art, omfang, formål og sammenheng 5](#_Toc182842103)

[Beskrivelse av dataflyt, personopplysningssikkerhet og ansvarsforhold 6](#_Toc182842104)

[Nødvendighet og proporsjonalitet 7](#_Toc182842105)

[Vurdering av personvernprinsippene 7](#_Toc182842106)

[Vurdering av de registrertes rettigheter og friheter 8](#_Toc182842107)

[Vurdering av de registrertes friheter 9](#_Toc182842108)

[Risikoer for de registrerte 10](#_Toc182842109)

[Risikoer relatert til åpenhet 10](#_Toc182842110)

[Risikoer relatert til medbestemmelse 10](#_Toc182842111)

[Risiko relatert til forutsigbarhet 10](#_Toc182842112)

[Andre risikoer 10](#_Toc182842113)

[Synspunkter fra interessentene 11](#_Toc182842114)

[Ledelsens validering 12](#_Toc182842115)

# Informasjon om gjennomføringen av DPIA

|  |
| --- |
| Informasjon |
| Navn på fagsystemet  |  |
| Leverandør av fagsystemet |  |
| Vurdering gjennomført dato |  |
| Vurdering gjennomført av |  |
| Er de registrerte involvert? (grunngi hvis ikke) |  |

# Innledende vurdering

*Dette kapitlet dokumenterer kommunens vurderinger av hvorvidt det foreligger høy risiko for de registrertes rettigheter og friheter, jf GDPR artikkel 35. Vurderingen tar utgangspunkt i vurderingskriterier som indikerer høy risiko. Dersom flere kriterier resulterer i ja, så kan det være behov for å gjennomføre DPIA.*

|  |  |
| --- | --- |
| Vurderingskriterier | Ja/Nei |
| Omfatter behandlingen evaluering eller poengsetting av de registrerte? |  |
| Omfatter behandlingen automatiserte avgjørelser med rettslig virkning? |  |
| Omfatter behandlingen en systematisk overvåking av de registrerte?  |  |
| Behandles særlige kategorier personopplysninger? |  |
| Behandles personopplysninger i stor skala? |  |
| Omfatter behandlingen matching eller sammenstilling av flere datasett?  |  |
| Omfatter behandlingen personopplysninger om sårbare registrerte (eksempelvis barn, pasienter, ansatte, eldre)? |  |
| Omfatter behandlingen innovativ bruk av teknologi eller organisatoriske verktøy, hvor tilknyttet risiko ennå ikke er kjent? |  |
| Hindrer behandlingen de registrerte i å utøve sine rettigheter? |  |

**Konklusjon fra den innledende vurderingen:**

**🗆** DPIA må gjennomføres

**🗆** DPIA må ikke gjennomføres

# Systematisk beskrivelse av behandlingen

*Dette kapitlet gir en systematisk beskrivelse av den planlagte behandlingen som skal utføres i fagsystemet. Beskrivelsen omfatter blant annet behandlingens art, omfang, formål og sammenheng behandlingen utføres i.*

## Beskrivelse av fagsystemet som behandlingen skal utføres i

|  |
| --- |
| Beskrivelse av fagsystemet |
| * Beskriv hovedfunksjonaliteten i fagsystemet
* Beskriv leverandøren som leverer fagsystemet
 |

## Beskrivelse av behandlingens art, omfang, formål og sammenheng

|  |
| --- |
| Beskrivelse av de registrerte og deres rettigheter |
| Om de registrerte, og om personopplysningene som samles inn* Beskriv hvem det samles inn personopplysninger om
* Beskriv hvilke personopplysninger som samles inn (eks navn, adresse)
* Beskriv hvordan personopplysningene samles inn (eks fra de registrerte selv)
* Beskriv om det samles inn personopplysninger fra sårbare registrerte (eks elever)
* Beskriv om det samles inn sensitive personopplysninger (eks helseopplysninger)
* Beskriv kommunens relasjon til de registrerte (tjenestemottakere etc)
* Anslå hvor mange registrerte som omfattes av behandlingen

Om de registrertes rettigheter* Beskriv hvordan de registrerte kan utøve sine rettigheter
* Beskriv i hvilken grad de registrerte har kontroll over egne personopplysninger
* Beskriv hvordan behandlingen vil oppfattes fra de registrertes perspektiv. Kan de registrerte oppfatte behandlingen som uforutsigbar?
* Beskriv om de registrerte har en særskilt forventning om konfidensialitet
* Beskriv om de registrerte har en særskilt forventning om at personopplysningene er nødvendige og korrekte
* Beskriv om de registrerte har en særskilt forventning om privatliv
 |

|  |
| --- |
| Beskrivelse av behandlingen |
| Om selve behandlingen* Beskriv hvordan personopplysningene skal brukes
* Beskriv hvor personopplysningene lagres
* Beskriv hvor lenge personopplysningene lagres
* Beskriv hvem som skal ha tilgang til personopplysningene
* Beskriv om behandlingen omfatter bruk av ny teknologi, hvor personvernkonsekvenser ikke har blitt vurdert
 |

|  |
| --- |
| Beskrivelse av behandlingsaktivitetene |
| Behandlingsaktivitet 1 | Beskriv formål | Ref artikkel 6 a-f |
| Behandlingsaktivitet 2 | Beskriv formål | Ref artikkel 6 a-f |
| Behandlingsaktivitet 3 | Beskriv formål | Ref artikkel 6 a-f |

## Beskrivelse av dataflyt, personopplysningssikkerhet og ansvarsforhold

|  |
| --- |
| Dataflyt, personopplysningssikkerhet og ansvarsforhold |
| Om databehandleren (dersom relevant)* Beskriv hvilke databehandlere som brukes.
* Beskriv hvilken databehandleravtale som er etablert.
* Beskriv hvilke garantier databehandlerne gir for at de gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at behandlingen gjennomføres i samsvar med personvernregelverket.

Om dataflyt* Beskriv alle kildene til personopplysningene, det vil si hvordan personopplysningene kommer inn i fagsystemet (skjema, integrasjoner).
* Beskriv alle mottakere av personopplysninger, det vil si hvordan personopplysninger sendes ut av fagsystemet (eksport, integrasjoner).

Om overføringer til tredjeland (dersom relevant)* Beskriv om personopplysningene overføres til land utenfor EU/EØS-området, og i så fall om det finnes adekvansvurderinger eller et annet gyldig overføringsgrunnlag.
* Dersom TIA er aktuelt, beskriv om TIA er gjennomført, inklusive landvurdering, og hvorvidt relevante sikkerhetstiltak er identifisert og gjennomført.

Om tekniske og organisatoriske sikkerhetstiltak* Beskriv hvordan personopplysningssikkerheten skal ivaretas i fagsystemet, herunder sikring av konfidensialitet, integritet, tilgjengelighet og robusthet (for eksempel sterk autentisering, kryptering, logging, overvåking, tilgangskontroll, sikkerhetsinstruks og taushetserklæring).
* Henvis gjerne til gjennomført ROS.

Om innebygd personvern* Beskriv hvordan fagsystemet ivaretar kravet til innebygd personvern.
 |

# Nødvendighet og proporsjonalitet

*Dette kapitlet dokumenterer kommunens vurderinger av hvorvidt behandlingen, og de enkelte behandlingsaktivitetene, er nødvendige og står i et rimelig forhold til formålet. Vurderingene omfatter en kvalitetssikring av hvorvidt fagsystemet oppfyller personvernprinsippene, og hvordan de registrertes rettigheter og friheter skal ivaretas.*

## Vurdering av personvernprinsippene

|  |
| --- |
| Lovlighet, rettferdighet og åpenhet |
| * Beskriv om behandlingen baseres på et tydelig behandlingsgrunnlag, og hvorvidt behandlingsgrunnlaget er gyldig og rimelig.
* Beskriv hvordan åpenhet skal ivaretas i behandlingen.
 |
| Formålsbegrensning |
| * Beskriv om formålet er klart definert.
* Beskriv om formålet samsvarer med forventningene til de registrerte.
* Beskriv om formålet kan oppnås med anonyme eller pseudonyme alternativer.
 |
| Dataminimering |
| * Beskriv om alle personopplysningene som samles inn er nødvendige for å oppnå formålet.
* Beskriv om det er mulig å begrense innsamlingen av personopplysninger.
* Beskriv om det er mulig å redusere detaljgraden av personopplysninger.
 |
| Riktighet |
| * Beskriv hvordan personopplysningene holdes korrekte og oppdaterte.
* Beskriv om de registrerte må involveres i å holde opplysningene korrekte.
* Beskriv hvorvidt det er behov for kontradiksjon, det vil si de registrertes anledning til å imøtegå det som den behandlingsansvarlige har registrert.
 |
| Lagringsbegrensning |
| * Beskriv hvordan personopplysningene slettes når formålet er nådd.
* Beskriv hvorvidt enkelte personopplysninger skal langtidsbevares og lagres i kommunens sak- og arkivsystem, jf riksarkivarens forskrift.
 |
| Integritet og konfidensialitet |
| * Beskriv om det er gjennomført en ROS av fagsystemet, jf artikkel 32. Gjør rede for eventuelle høye risikoer som ikke kan reduseres med sikkerhetstiltak, og som bør vurderes i denne DPIAen.
* Beskriv om personopplysningssikkerheten er tilstrekkelig ivaretatt.
 |

## Vurdering av de registrertes rettigheter og friheter

|  |
| --- |
| Rett til informasjon |
| * Beskriv hvordan informasjon om behandlingen skal gis de registrerte (eks personvernerklæringer, eller annen informasjon i fagsystemet).
 |
| Rett til innsyn |
| * Beskriv hvordan de registrerte skal utøve retten til innsyn i egne personopplysninger (eks profilside i fagsystemet, eller skjema for innsynsforespørsel).
 |
| Rett til retting |
| * Beskriv om det skal være mulig for de registrerte å korrigere sine egne personopplysninger, og i så fall hvordan de registrerte kan utøve denne rettigheten.
 |
| Rett til sletting |
| * Beskriv om det skal være mulig for de registrerte å slette sine egne personopplysninger, og i så fall hvordan de registrerte kan utøve denne rettigheten.
 |
| Rett til begrensning |
| * Beskriv om det skal være mulig for de registrerte å utøve retten til å begrense behandlingen til egne personopplysninger, og i så fall hvordan de registrerte kan utøve denne rettigheten.
 |
| Rett til dataportabilitet |
| * Beskriv om det skal være mulig for de registrerte å utøve retten til dataportabilitet, og i så fall hvordan de registrerte kan utøve denne rettigheten.
 |
| Rett til å protestere |
| * Beskriv om det skal være mulig for de registrerte å utøve retten til å protestere, og i så fall hvordan de registrerte kan utøve denne rettigheten.
 |
| Rettigheter ved automatiserte avgjørelser og profilering |
| * Beskriv om det gjennomføres automatiserte avgjørelser og profilering av de registrerte. Beskriv i så fall hvordan de registrerte kan utøve denne rettigheten.
 |

## Vurdering av de registrertes friheter

|  |
| --- |
| Vurderinger rundt de registrertes friheter i forhold til Den europeiske menneskerettskonvensjonen (EMK) |
| * Beskriv hvordan behandlingen tar hensyn til retten til privatliv og kommunikasjonsvern
* Beskriv hvordan behandlingen tar hensyn til retten til å ikke bli diskriminert
* Beskriv hvordan behandlingen tar hensyn til retten til tanke-, tros- og religionsfrihet
* Beskriv hvordan behandlingen tar hensyn til retten til ytrings- og informasjonsfrihet
 |

# Risikoer for de registrerte

*Dette kapitlet dokumenterer kommunens vurderinger av personvernkonsekvenser for de registrertes rettigheter, samt relevante tiltak for å redusere disse konsekvensene. Vurderingene tar utgangspunkt i de registrertes perspektiv, og omfatter blant annet vurderinger av risikoer for manglende reell åpenhet, medbestemmelse og forutsigbarhet. Dette gjøres for å kontrollere om behandlingen kan gjennomføres på en måte som er akseptabel og tillitsskapende ovenfor de registrerte.*

## Risikoer relatert til åpenhet

Åpenhet omfatter risikoer og tiltak relatert til informasjon og innsyn.

|  |  |  |  |
| --- | --- | --- | --- |
| Beskriv uønsket hendelse (risikoscenario) | Beskriv risiko (høy, middels, lav) | Beskriv planlagte tiltak | Beskriv risiko etter tiltak (høy, middels, lav) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Risikoer relatert til medbestemmelse

Medbestemmelse omfatter risikoer og tiltak relatert til de registrertes rettigheter etter personvernregelverket.

|  |  |  |  |
| --- | --- | --- | --- |
| Beskriv uønsket hendelse (risikoscenario) | Beskriv risiko (høy, middels, lav) | Beskriv planlagte tiltak | Beskriv risiko etter tiltak (høy, middels, lav) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Risiko relatert til forutsigbarhet

Forutsigbarhet omfatter risikoer og tiltak relatert til å gjøre behandlingsaktivitetene mindre komplekse, og dermed lettere å forstå.

|  |  |  |  |
| --- | --- | --- | --- |
| Beskriv uønsket hendelse (risikoscenario) | Beskriv risiko (høy, middels, lav) | Beskriv planlagte tiltak | Beskriv risiko etter tiltak (høy, middels, lav) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Andre risikoer

Andre risikoer kan være relatert til vurderinger av personvernprinsippene, de registrertes rettigheter. høye risikoer som er dekket av ROS, samt rettigheter og friheter etter EMK.

|  |  |  |  |
| --- | --- | --- | --- |
| Beskriv uønsket hendelse (risikoscenario) | Beskriv risiko (høy, middels, lav) | Beskriv planlagte tiltak | Beskriv risiko etter tiltak (høy, middels, lav) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Synspunkter fra interessentene

*I dette kapitlet skal skolen sammenfatte synspunktene til personvernombudet og, dersom relevant, de registrerte.*

|  |
| --- |
| Personvernombudets råd og anbefalinger  |
| * Beskriv personvernombudets vurdering av behandlingen.
* Beskriv personvernombudets vurdering av om restrisikoen er akseptabel.
 |

|  |
| --- |
| De registrertes synspunkter på behandlingen  |
| * Beskriv de registrertes vurdering behandlingen.
* Beskriv de registrertes vurdering av om restrisiko er akseptabel.
 |

# Ledelsens validering

*Dette kapitlet gir et sammendrag av DPIAen, en innstilling til ledelsen, samt ledelsens vurderinger og beslutning.*

|  |
| --- |
| Sammendrag og anbefaling til ledelsen |
| * Skriv et sammendrag av vurderingene som er gjort, herunder det samlede risikobildet, de planlagte tiltakene og eventuell restrisiko.
* Skriv en innstilling til ledelsen (konklusjon fra arbeidsgruppa).
 |

|  |
| --- |
| Ledelsens vurderinger |
| * Skriv når og i hvilket møte ledelsen har behandlet DPIAen.
* Skriv hvilke vurderinger ledelsen har gjort.
 |

|  |
| --- |
| Ledelsens beslutning |
|

|  |  |
| --- | --- |
| 🗆 | Risikoen for de registrertes rettigheter og friheter er redusert til et akseptabelt nivå. Når tiltak er implementert kan behandlingen gjennomføres. |
| 🗆 | Risikoen for de registrertes rettigheter og friheter er ikke redusert til et akseptabelt nivå. Behandlingen kan ikke gjennomføres. |
| 🗆 | Risikoen for de registrertes rettigheter og friheter er ikke redusert til et akseptabelt nivå. Forhåndsdrøfting med Datatilsynet må gjennomføres før ledelsen tar en beslutning om behandlingen. |

 |