

**[VIRKSOMHET]**

**[Tittel på løsning/systemer/endringer/]**

**Dato for vurdering: [xx.xx.xxxx]**

Mal: april 2022

Innledende personvernvurdering (IP)

**Om vurderingen**

Virksomheter i Oslo kommune må vurdere ulike personvernsaspekter før behandling av personopplysninger starter. Hensikten med denne innledende personvernvurderingen (IP) er å kartlegge grunnleggende data/informasjon knyttet til behandlingen og overordnet å vurdere risikoen for den registrerte.

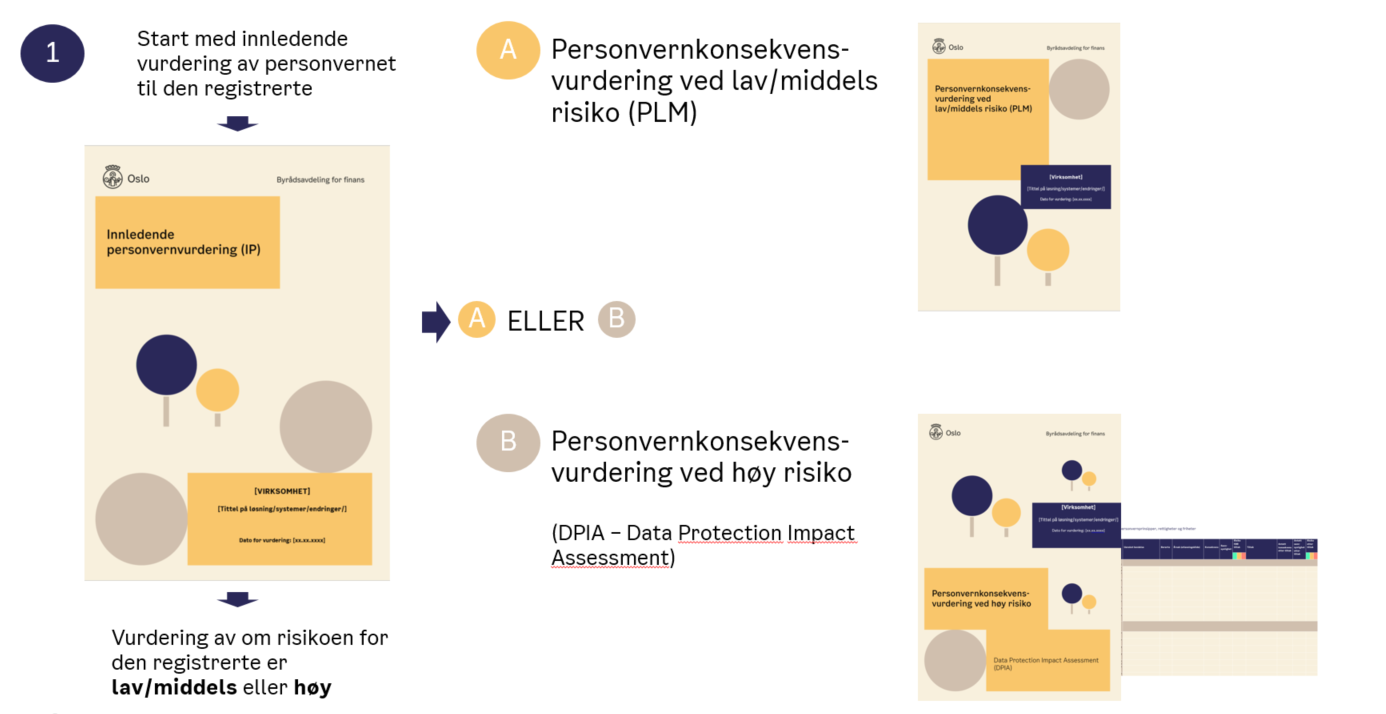
Behandlingsansvarlig må ha kontroll over all sin behandling av personopplysninger. Dette innebærer at behandlingsansvarlig må ha en systematisk beskrivelse av sine planlagte behandlinger. IP er ment som en kartlegging av grunnleggende informasjon ved behandlingen, for å sikre at virksomhetene har en slik systematisk beskrivelse på plass. Innholdet i IP vil også være relevant for oversikt over behandling av personopplysninger (behandlingsoversikt/protokoll), personvernerklæringer, ved avvikshåndtering og i kontakt med den registrerte. Noen av de nødvendige vurderinger som må gjøres etter personvernregelverket vil også ivaretas.

Det vil alltid være en risiko ved behandling av personopplysninger. Kravene i personvernregelverket gjelder uavhengig av risikonivå, og dette vil si at virksomheter alltid må vurdere personvernsaspekter av behandling av personopplysninger selv om risikoen er lav. Dersom denne vurderingen viser at personvernrisikoen er lav/middels, må virksomheten gjøre en *Personvernkonsekvensvurdering ved lav/middels risiko (PLM).* Dersom risikoen er høy, må det gjøres en DPIA (*Personvernkonsekvensvurdering ved høy risiko*).

IP trenger kun korte svar på spørsmålene.

Spørsmålene i IP kapittel 1-5, kommer igjen i de utvidede vurderingene (PLM og DPIA). Siden vurderingene brukes videre, vil en grundig vurdering i IP gjøre arbeidet med PLM eller DPIA enklere og mer effektivt.

Det er utarbeidet en egen [Veileder til IP, PLM og DPIA med tilhørende begrepsliste](https://felles.intranett.oslo.kommune.no/informasjonssikkerhet-og-personvern/personvern/veiledninger-og-maler/dpia/). Disse dokumentene er ment å være til hjelp i gjennomføring av vurderingen.



Bilde 1: Skisse av vurderingsprosessen.

Innhold

[1. Grunnleggende informasjon om tjeneste/løsning/system/prosess og roller 5](#_Toc102387478)

[2. Grunnleggende informasjon om de registrerte 5](#_Toc102387479)

[3. Grunnleggende informasjon om personopplysninger 6](#_Toc102387480)

[4. Grunnleggende informasjon om planlagt behandling 8](#_Toc102387481)

[5. Grunnleggende informasjon om formål 10](#_Toc102387482)

[6. Særlig plikter og unntak etter GDPR art. 35 11](#_Toc102387483)

[7. Grunnleggende informasjon om behov for DPIA 11](#_Toc102387484)

[8. Konklusjon 13](#_Toc102387485)

[9. Involvering og godkjenning 14](#_Toc102387486)

# Grunnleggende informasjon om tjeneste/løsning/system/prosess og roller

|  |  |  |
| --- | --- | --- |
|  | | |
| Navn på tjeneste/løsning/system/prosess | |  |
| Virksomhetstilhørighet *[i hvilke virksomheter skal behandlingen skje?]* | |  |
| Behandlingsansvarlig  Ved felles behandlingsansvar, skriv alle behandlingsansvarlige | |  |
| Kontaktpersoner hos behandlingsansvarlig | | [Navn, rolle/funksjon] |
| Systemeier/løsningseier/prosjekteier (risikoeier) | |  |
| Systemforvalter | |  |
| Databehandler | |  |
| **Vurdering utført av (deltakere)** | | |
| [Navn] | [Rolle/funksjon] | |
| [Navn] | [Rolle/funksjon] | |
| [Navn] | [Rolle/funksjon] | |

# Grunnleggende informasjon om de registrerte

|  |  |
| --- | --- |
|  | |
| Hvem er de registrerte?  *[Velg de aktuelle]* | Ansatte i egen virksomhet eller i Oslo kommune generelt  Kunder/klienter/brukere/leietakere  Innbyggere generelt  Barnehagebarn/elever/studenter  Pasienter  Eldre (personer over 67 år)  Barn  Under 12 år  12-15 år  16-18 år  Personer med funksjonsnedsettelse  Personer tildelt eller innvilget kode 4, 6 og 7 etter folkeregisterloven |
|  | Andre sårbare registrerte, spesifiser:  Klikk her for å skrive inn tekst. |
|  | Andre:  Klikk her for å skrive inn tekst. |

# Grunnleggende informasjon om personopplysninger

|  |  |
| --- | --- |
|  | |
| Hvilke typer personopplysninger skal behandles? | Alminnelige personopplysninger (GDPR art. 4 nr. 1)  Særlige kategorier personopplysninger (GDPR art. 9 nr. 1)  Personopplysninger om straffedommer og lovovertredelser eller tilknyttede sikkerhetstiltak (GDPR art. 10)  Andre personopplysninger av følsom karakter for de registrerte (som ikke er særlige kategorier personopplysninger) |
| Hvilke alminnelige personopplysninger skal behandles? | Navn  Adresse  E-post  Telefonnummer  Fødselsdato  Sivilstatus  Yrke  Utdanning  Andre alminnelige personopplysninger |
| Hvilke særlige kategorier personopplysninger skal behandles? | Rasemessig eller etnisk opprinnelse  Politisk oppfatning, religion eller filosofisk overbevisning  Fagforeningsmedlemskap  Genetiske eller biometriske opplysninger  Helseopplysninger  Seksuelle forhold eller seksuell orientering |
| Beskriv nærmere hvilke særlige kategorier personopplysninger som skal behandles: | |
|  | |

# Grunnleggende informasjon om planlagt behandling

|  |  |
| --- | --- |
|  | |
| Hvor mange registrerte skal det behandles personopplysninger om? | [tall eller prosent] |
| Hvordan skal personopplysningene behandles? | innsamling  lagring  sletting  retting  aksess/gi tilgang  deling/utlevering  tilgjengeliggjøring  motta  sammenstilling  annet:  Klikk her for å skrive inn tekst. |
| Hvordan skal personopplysningene samles inn? | Personopplysningene hentes direkte fra de registrerte  Personopplysningene hentes fra datakilde innenfor Oslo kommune  Personopplysningene hentes fra datakilde utenfor Oslo kommune  Annet  Klikk her for å skrive inn tekst. |
| Hvor lenge skal personopplysningene lagres? | Antall dager/måneder/år eller annen tidfesting |
| Skal personopplysningene kunne slettes? | Ja  Nei |
| Skal personopplysningene kunne rettes? | Ja  Nei |
| Hvem skal ha tilgang til personopplysningene? | Kun behandlingsansvarlig og databehandler  Andre med tjenstlig behov i Oslo kommune f.eks. IT-personell, saksbehandler ol.  Andre  Klikk her for å skrive inn tekst. |

|  |  |
| --- | --- |
| Skal personopplysningene deles med, utleveres eller tilgjengeliggjøres til andre *virksomheter* i eller utenfor Oslo kommune? | Nei  Ja, deles med/utleveres/ tilgjengeliggjøres til:  Virksomheter innenfor Oslo kommune  Virksomheter eller personer utenfor Oslo kommune  Offentlige organer, tilsynsmyndigheter ol.  Politi eller påtalemyndighet  Privat virksomhet  Andre  Klikk her for å skrive inn tekst. |

|  |  |
| --- | --- |
| Skal personopplysningene deles med, utleveres eller tilgjengeliggjøres til *personer* utenfor Oslo kommune? | Nei  Ja, deles med/utleveres/ tilgjengeliggjøres til:  Alle innbyggere  Alle innloggede brukere  Personer med partsinteresse  Foreldre til barn:  Under 12 år  12-15 år  16-18 år  Verger eller fullmektiger  Pårørende  Andre  Klikk her for å skrive inn tekst. |

# Grunnleggende informasjon om formål

|  |  |
| --- | --- |
|  | |
| Hva er formålet med behandlingen av personopplysninger? |  |
| Skal personopplysninger viderebehandles eller innebærer behandlingen av personopplysninger en viderebehandling?  Hvis ja, hva er formålet med viderebehandling av personopplysninger (nytt formål)? | Nei  Ja  Klikk her for å skrive inn tekst. |
| Ved viderebehandling av personopplysninger, hva er det opprinnelige formålet med behandlingen? |  |

# Særlig plikter og unntak etter GDPR art. 35

|  |  |
| --- | --- |
|  | |
| Det skal gjennomføres DPIA etter GDPR art. 35 nr. 3 i følgende tilfeller:   1. En systematisk og omfattende vurdering av personlige aspekter av de registrerte som er basert på automatisert behandling, herunder profilering, og som danner grunnlag for avgjørelser som har rettsvirkning for de registrerte eller på lignende måte i betydelig grad påvirker den registrerte 2. Behandling i stor skala av særlige kategorier personopplysninger (GDPR art. 9 nr. 1) eller av personopplysninger om straffedommer og lovovertredelser (GDPR art. 10) 3. En systematisk overvåking i stor skala av et offentlig tilgjengelig område | |
| Kan den planlagte behandlingen anses som et av tilfellene nevnt ovenfor? | Ja, spesifiser hvilket tilfelle a, b eller c  Velg et element.  Nei |
| Det skal *ikke* være nødvendig å gjennomføre DPIA etter GDPR art. 35 nr. 10 dersom:   * behandlingen er i henhold til GDPR art. 6 nr. 1 bokstav c) eller e) har et rettslig grunnlag i loven som virksomhetene er underlagt, og * nevnte lov regulerer den eller de aktuelle spesifikke behandlingsaktivitetene, og * det allerede er utført en vurdering av personvernkonsekvenser som en del av en generell personvernvurdering i forbindelse med vedtakelse av loven. | |
| Kan den planlagte behandlingen anses som dekket av unntaket som nevnt ovenfor? | Ja  Nei |

# Grunnleggende informasjon om behov for DPIA

*For å finne riktig svar i dette kapitlet, se Veileder til IP, PLM og DPIA for beskrivelser og eksempler for de enkelte punktene. Se også Begrepsliste til IP, PLM og DPIA for en beskrivelse/forklaring av begreper som brukes i de enkelte punktene.*

|  |  |  |
| --- | --- | --- |
|  |  | **Ja/Nei** |
|  | Behandling av:   * særlige kategorier personopplysninger (GDPR art. 9) * personopplysninger om straffbare forhold/dommer (GDPR art. 10) * andre personopplysninger av følsom karakter for den registrerte | Velg et element. |
|  | Behandling av personopplysninger i «stor skala» (antall registrerte i tall eller andel, volumet av data, lagringstid eller geografisk omfang). | Velg et element. |
|  | Behandling av personopplysningene på nye måter som kan oppfattes som inngripende for personvernet eller ikke forutsigbart for den registrerte. | Velg et element. |
|  | Behandlingen vil føre til beslutninger eller tiltak med betydelig innvirkning på enkeltpersoner eller de registrerte selv f.eks. vedtak, tjenestenekt osv. | Velg et element. |
|  | Behandlingen vil innebære at de registrerte kontaktes på måter som de kan finne inngripende. | Velg et element. |
|  | Evaluering eller scoring/profilering i stor skala f. eks. for å forutsi den registrertes antatte evner eller egenskaper. | Velg et element. |
|  | Automatiserte beslutningsprosesser med rettslige eller lignende vesentlige konsekvenser for den registrerte. | Velg et element. |
|  | Systematisk overvåkning eller sporing av en persons geografiske posisjon eller atferd, f.eks. på internett. | Velg et element. |
|  | Matching eller sammenstilling av data fra flere kilder, dvs. at det kombineres, sammenlignes eller avstemmes personopplysninger fra flere kilder. | Velg et element. |
|  | Opplysninger om sårbare registrerte personer eller ubalanse i styrkeforhold. | Velg et element. |
|  | Innovativ bruk av eksisterende teknologi eller organisatoriske løsninger, eller bruk av nye teknologiske eller nye organisatoriske løsninger (herunder bruk av biometriske og/eller genetiske opplysninger). | Velg et element. |
|  | Behandlingsansvarlig henter inn personopplysningene fra andre enn den registrerte selv, og den registrerte har derfor ikke mulighet til å vite at opplysningene blir behandlet. | Velg et element. |
|  | Bruk av personopplysninger om barn til informasjons- eller markedsføringsformål (eventuelt basert på automatisert utvalg), eller dersom virksomheten planlegger å tilby nettjenester direkte til barn. | Velg et element. |
|  | Behandling av personopplysninger i land utenfor EU/EØS (tredjeland) som ikke er godkjent av EU-kommisjonen. | Velg et element. |

Dersom svaret er «ja» på ett eller flere av spørsmålene ovenfor, kan det bety at det foreligger «høy risiko» og behov for DPIA. Det må gjøres en konkret vurdering av svarene på alle spørsmålene i denne malen (ikke bare spørsmål i kapittel VII) for å avgjøre om det foreligger høy risiko.

Dersom det er usikkerhet rundt hvilken personvernvurdering (PLM eller DPIA) som skal gjennomføres, bør det gjennomføres en DPIA.

# Konklusjon

|  |  |
| --- | --- |
|  | |
| Oppsummering av funn: | Det foreligger ikke høy risiko  Det foreligger høy risiko |
| Beskriv funn som tilsier høy risiko: |  |
| Foreligger det plikt til å gjennomføre DPIA etter GDPR art. 35? | Ja  Nei |
| Foreligger det unntak fra å gjennomføre DPIA etter GDPR art. 35? | Ja  Nei |
| Hvilken personvernvurdering må gjennomføres? | PLM  DPIA |

# Involvering og godkjenning

|  |  |
| --- | --- |
|  | |
| Vurderingen er sluttført av | [Navn] og [dato] |
| Involvering (hvis nødvendig) av f.eks. personvernombudet eller sentralt fagmiljø for personvern og informasjonssikkerhet i Oslo kommune (FIN/ISI).  *[Personvernombudet og FIN/ISI skal ikke gjennomføre denne vurderingen, og deres involvering er kun ment som veiledning til konkrete spørsmål og kan ikke anses som en godkjenning av vurderingen.]* | [Navn og rolle] og [dato] |
| Godkjenning fra behandlingsansvarlig | [Navn] og [godkjenningsdato] |
| Godkjenning fra andre aktuelle roller f. eks. systemeier/løsningseier/prosjekteier (risikoeier). | [Navn] og [godkjenningsdato] |