

**[Virksomhet]**

[Tittel på løsning/systemer/endringer/]

Dato for vurdering: [xx.xx.xxxx]

Mal: mal 2022

Personvernkonsekvensvurdering ved lav/middels risiko (PLM)

**Om vurderingen**

Virksomheter i Oslo kommune må vurdere ulike personvernsaspekter før behandling av personopplysninger starter. 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.

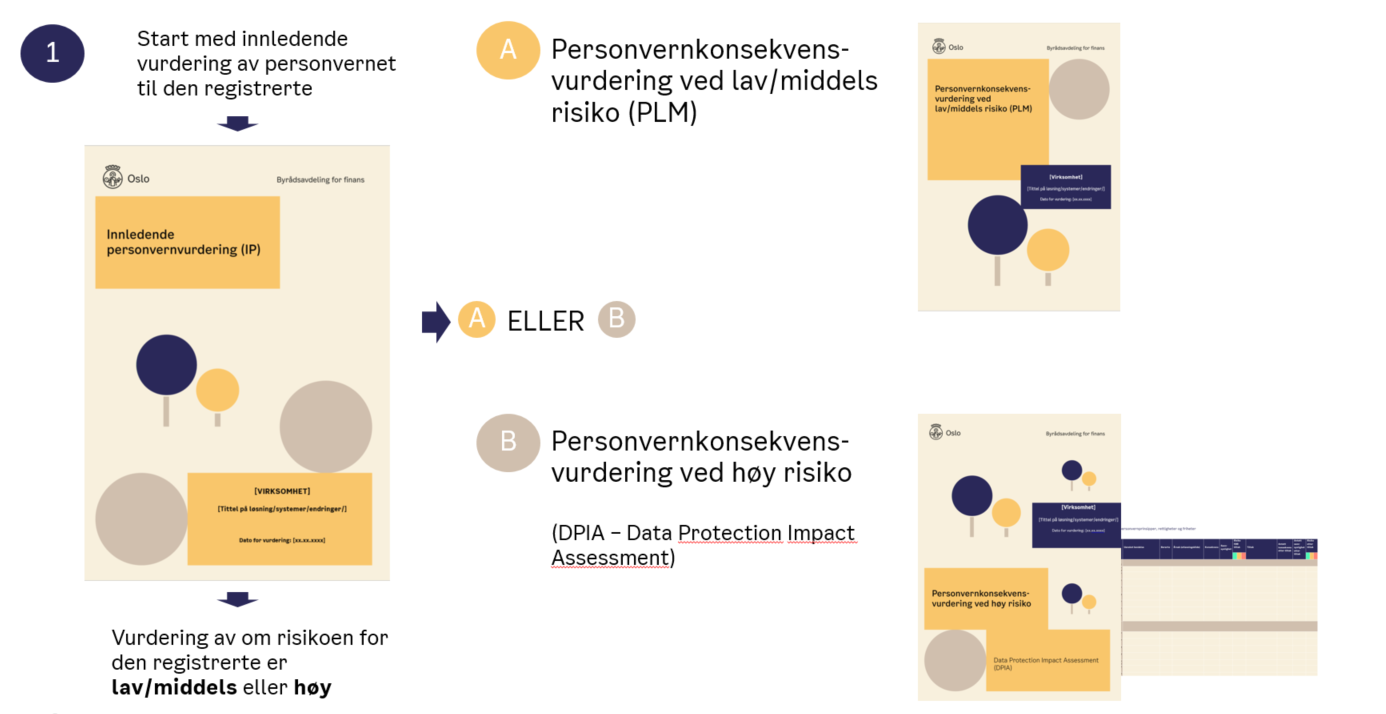
På bakgrunn av konklusjonen i *Innledende personvernvurdering (IP)* skal virksomheten gjennomføre enten *Personvernkonsekvensvurdering ved lav/middels risiko (PLM)* eller *Personvernkonsekvensvurdering ved høy risiko, DPIA.*

Hensikten med PLM er å sikre at virksomheten har oversikt over hvilke konsekvenser den planlagte behandlingen vil ha for personvernet, sørge for at de registrertes rettigheter og friheter blir ivaretatt og bidra til at virksomheten etterlever kravene i regelverket for behandling av personopplysninger.

Spørsmålene i PLM kapittel 1-5 tilsvarer spørsmålene i IP kapittel 1-5, men er utvidet med noen flere spørsmål. Der spørsmålene er likelydende som i IP, brukes svarene fra IP her. En grundig vurdering i IP vil gjøre arbeidet med PLM enklere og mer effektivt.

Det er viktig at virksomhetene gjennomgår og vurderer alle spørsmålene, selv om ikke alle spørsmål er like relevant for enhver behandling av personopplysninger. Dette for å sikre at alle aspekter ved behandlingen er vurdert, samt at det vil gi virksomhetene en oversikt over hva de kan eller ikke kan gjøre med personopplysningene. PLM vil på denne måten bidra til at virksomhetene oppfyller ansvarlighetsprinsippet i personvernregelverket.

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](#_Toc102387358)

[2. Grunnleggende informasjon om de registrerte 5](#_Toc102387359)

[3. Grunnleggende informasjon om personopplysninger 6](#_Toc102387360)

[4. Behandlingens art, omfang og kontekst 8](#_Toc102387361)

[4A. Beskrivelse av behandlingen 8](#_Toc102387362)

[4B. Behandlingens art 8](#_Toc102387363)

[4C. Behandlingens omfang 11](#_Toc102387364)

[4D. Behandlingens kontekst 11](#_Toc102387365)

[4E. Overføring til utlandet 12](#_Toc102387366)

[5. Behandlingens formål 13](#_Toc102387367)

[5A. Formål for førstegangsbehandling 13](#_Toc102387368)

[5B. Formål ved viderebehandling 13](#_Toc102387369)

[6. Behandlingens lovlighet 14](#_Toc102387370)

[6A. Behandlingsgrunnlag 14](#_Toc102387371)

[6B. Samtykke 16](#_Toc102387372)

[7. Behandlingens nødvendighet og proporsjonalitet 17](#_Toc102387373)

[7A. Nødvendighetsvurdering 17](#_Toc102387374)

[7B. Proporsjonalitetsvurdering 17](#_Toc102387375)

[7C. Ivaretakelse av personvernprinsippene 17](#_Toc102387376)

[7D. Ivaretakelse av de registrertes rettigheter 18](#_Toc102387377)

[7E. Ivaretakelse av de registrertes friheter 20](#_Toc102387378)

[7F. Databehandlere 20](#_Toc102387379)

[8. Risiko og tiltak 21](#_Toc102387380)

[8A. Personopplysningssikkerhetsrisiko 22](#_Toc102387381)

[8B. Annen personvernrisiko 23](#_Toc102387382)

[9. Involvering, risikoaksept og godkjenning 23](#_Toc102387383)

**Vedlegg X**: Risikoanalyse for personvernrisiko

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

Spørsmålene i PLM kapittel 1 er tilsvarende som i IP kapittel 1, men er her utvidet med flere spørsmål.

|  |  |  |
| --- | --- | --- |
|  | | |
| Navn på tjeneste/løsning/system | |  |
| 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] | |
| [Navn på ressurs som har deltatt i ROS] | [Rolle/funksjon] | |

# Grunnleggende informasjon om de registrerte

Spørsmålet i PLM kapittel 2 er tilsvarende som i IP kapittel 2.

|  |  |
| --- | --- |
|  | |
| 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

Spørsmålene i PLM kapittel 3 er tilsvarende som i IP kapittel 3, men er her utvidet med flere spørsmål.

|  |  |
| --- | --- |
|  | |
| 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: |
|  |

# Behandlingens art, omfang og kontekst

Spørsmålene i PLM kapittel 4 går igjen fra IP kapittel 4, men er her utvidet med flere spørsmål.

## 4A. Beskrivelse av behandlingen

Beskriv prosessene for behandling av personopplysninger i løsning, tjeneste og system (inkl. data- og informasjonsflyt). Beskrivelsen bør omfatte hele livssyklusen til personopplysninger (fra innsamling til sletting). I tillegg bør løsning, tjeneste og system beskrives her. Legg eventuelt ved løsningsbeskrivelser eller skisser, dersom dette finnes.

|  |
| --- |
|  |

## 4B. Behandlingens art

|  |  |
| --- | --- |
|  | |
| Hvordan skal personopplysningene behandles? | innsamling  lagring  sletting  retting  aksess/gi tilgang til  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 rettes? | Ja  Nei |
| Skal personopplysningene kunne slettes? | 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. |

## 4C. Behandlingens omfang

|  |  |
| --- | --- |
|  | |
| Hvor mange registrerte skal det behandles personopplysninger om? | [tall eller prosent] |
| Hvor store mengder personopplysninger skal behandles? | [tall eller prosent]  Hvis det ikke det er mulig å tallfeste mengder av personopplysninger, forklar mengden ved å bruke f.eks. antall variabler e.l. |
| Beskriv andre momenter som har betydning for behandlingens omfang (f. eks. om det behandles flere kategorier av personopplysninger, volum av personopplysninger, geografisk omfang osv.): | |
|  | |

## 4D. Behandlingens kontekst

|  |  |
| --- | --- |
|  | |
| Har de registrerte kontroll over sine personopplysninger? | Nei  Ja, beskriv under |
|  | |
| Vil de registrerte ha en *særskilt forventning* til kommunen ved behandling av personopplysninger (f. eks. innenfor helse- og omsorgstjenesten?) | Nei  Ja, beskriv under |
|  | |
| Er det ujevnt maktforhold mellom behandlingsansvarlige og de registrerte? | Nei  Ja, beskriv under |
|  | |
| Behandles personopplysninger fra ulike datasett og kilder i og/eller utenfor Oslo kommune? | Nei  Ja, beskriv under |
|  | |
| Behandles personopplysninger fra ulike behandlingsansvarlige i og/eller utenfor Oslo kommune? | Nei  Ja, beskriv under |
|  | |
| Beskriv andre momenter som kan påvirke rimelige forventninger fra de registrerte eller påvirke konsekvenser av behandlingen av personopplysninger: | |
|  | |

## 4E. Overføring til utlandet

|  |  |
| --- | --- |
|  | |
| **Overføring av personopplysningene til land innenfor EU/EØS og land utenfor EU/EØS (tredjeland) som er godkjent av EU-kommisjonen.**  *Dette inkluderer utlevering av personopplysninger til en annen behandlingsansvarlig eller myndighet i utlandet. Bruk av utenlandske databehandlere og underdatabehandlere som behandler personopplysninger medfører også overføring til utlandet.* | |
| Er det planlagt å overføre personopplysninger til land innenfor EU/EØS? | Nei  Ja  Angi til hvilket land |
| Er det planlagt å overføre personopplysninger til land utenfor EU/EØS (tredjeland) som er godkjent av EU-kommisjonen? | Nei  Ja  Angi til hvilket land |

# Behandlingens formål

Spørsmålene i PLM kapittel 5 går igjen fra IP kapittel 5, men er her utvidet med flere spørsmål.

Hvis det er snakk om førstegangsbehandling, gå til punkt A. Hvis det er snakk om viderebehandling, gå til punkt B.

## 5A. Formål for førstegangsbehandling

|  |
| --- |
|  |
| Beskriv formålet med behandlingen av personopplysningene. Formålene må være spesifikke, uttrykkelig angitte og berettigede. Dersom det er flere behandlingsaktiviteter med ulike formål, skal alle formålene listes opp. |
|  |

## 5B. Formål ved viderebehandling

|  |  |
| --- | --- |
|  | |
| Hva er formålet med viderebehandling av personopplysningene (nytt formål)? |  |
| Hva er det opprinnelige formålet med behandlingen? |  |
| Er det forenlighet mellom det nye formålet og det opprinnelige formålet? | Nei  Ja, beskriv under |
|  | |

# Behandlingens lovlighet

## 6A. Behandlingsgrunnlag

|  |  |
| --- | --- |
|  | |
| Har behandlingen av personopplysninger behandlingsgrunnlag i GDPR?  *[For å finne riktig behandlingsgrunnlag, se Veileder om behandlingsgrunnlag]* | |
| **Behandlingsgrunnlag for alminnelige personopplysninger etter GDPR art. 6** | **Behandlingsgrunnlag for særlige kategorier personopplysninger etter GDPR art. 9** |
| a. Samtykke | a. Samtykke |
| b. Avtale | b. Forpliktelser og rettigheter for den behandlingsansvarlige eller den registrerte på området arbeidsrett, trygderett og sosialrett.  *[Dette behandlingsgrunnlaget vil kreve supplerende rettsgrunnlag.]* |
| c. Rettslig forpliktelse  *[Dette behandlingsgrunnlaget vil kreve supplerende rettsgrunnlag.]* | c. Vitale interesser til den registrerte eller en annen fysisk person, dersom samtykke ikke kan gis |
| d. Vitale interesser til den registrerte eller en annen fysisk person | d. Behandlingen utføres av en stiftelse, sammenslutning eller et annet ideelt organ hvis mål er av politisk, religiøs eller fagforeningsmessig art |
| e. Allmennhetens interesse eller utøvelse av offentlig myndighet som den behandlingsansvarlige er pålagt.  *[Dette behandlingsgrunnlaget vil kreve supplerende rettsgrunnlag.]* | e. Behandlingen gjelder personopplysninger som det er åpenbart at den registrerte har offentliggjort |
| f. Berettiget interesse som forfølges av den behandlingsansvarlige eller en tredjepart.  *[Dette behandlingsgrunnlaget vil kreve en interesseavveiing.]* | f. For å fastsette, gjøre gjeldende eller forsvare rettskrav eller når domstolene handler innenfor rammene av sin domsmyndighet |
|  | g. Viktige allmenne interesser  *[Dette behandlingsgrunnlaget vil kreve supplerende rettsgrunnlag.]* |
|  | h. Behandlingen i forbindelse med forebyggende medisin eller arbeidsmedisin for å vurdere en arbeidstakers arbeidskapasitet, i forbindelse med medisinsk diagnostikk, yting av helse- eller omsorgstjenester, behandling eller forvaltning av helse- eller sosialtjenester og –systemer.  *[Dette behandlingsgrunnlaget vil kreve supplerende rettsgrunnlag.]* |
|  | i. Allmenne folkehelsehensyn eller for å sikre høye kvalitets- og sikkerhetsstandarder for helsetjenester og legemidler eller medisinsk utstyr.  *[Dette behandlingsgrunnlaget vil kreve supplerende rettsgrunnlag.]* |
|  | j. Arkivformål i allmennhetens interesse eller formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål.  *[Dette behandlingsgrunnlaget vil kreve supplerende rettsgrunnlag.]* |
| Angi supplerende rettsgrunnlag (hvis aktuelt): | |
|  | |

## 6B. Samtykke

*Denne delen besvares kun dersom samtykke brukes som behandlingsgrunnlag.*

|  |  |
| --- | --- |
|  | |
| Bekreft hvilke av samtykkekravene som er oppfylt. *[Kryss av]*  (GDPR art. 4 nr. 11 og art. 7)  *[Alle kravene må være oppfylt for at samtykket skal være gyldig]* | Frivillig  Spesifikt  Informert  Utvetydig |
| Er samtykket dokumentert?   (GDPR art. 7 nr. 1) | Ja  Nei |
| Gis samtykke i forståelig og lett tilgjengelig form på et klart og enkelt språk?  (GDPR art. 7 nr. 2) | Ja  Nei |
| Er det like enkelt å trekke tilbake samtykke som å gi?   (GDPR art. 7 nr. 3) | Ja  Nei |
| Andre momenter [beskriv problemstillinger, momenter eller merknader knyttet til bruk av samtykke]: | |
|  | |

# Behandlingens nødvendighet og proporsjonalitet

## 7A. Nødvendighetsvurdering

|  |  |
| --- | --- |
|  | |
| Oppnås det faktiske formålet med behandlingen? | Ja  Nei, beskriv under |
|  | |
| Kan formålet oppnås uten at personopplysninger blir behandlet? | Nei  Ja, beskriv under |
|  | |

## 7B. Proporsjonalitetsvurdering

|  |  |
| --- | --- |
|  | |
| Er det et rimelig forhold mellom inngrepet som gjøres i personvernet og de fordelene som oppnås ved behandlingen? | Nei  Ja, beskriv under |
|  | |

## 7C. Ivaretakelse av personvernprinsippene

|  |  |
| --- | --- |
|  | |
| *Beskriv hvordan alle prinsippene for behandling av personopplysninger ivaretas.* | |
| Lovlighet, rettferdighet og åpenhet  (GDPR art. 5 nr. 1 bokstav a) | *[For å fylle ut dette punktet, se vurderingsmomenter for prinsippet om lovlighet, rettferdighet og åpenhet i Veileder til IP, PLM og DPIA]* |
| Formålsbegrensning  (GDPR art. 5 nr. 1 bokstav b) | *[For å fylle ut dette punktet, se vurderingsmomenter for prinsippet om formålsbegrensning i Veileder til IP, PLM og DPIA]* |
| Dataminimering  (GDPR art. 5 nr. 1 bokstav c) | *[For å fylle ut dette punktet, se vurderingsmomenter for prinsippet om dataminimering i Veileder til IP, PLM og DPIA]* |
| Riktighet  (GDPR art. 5 nr. 1 bokstav d) | *[For å fylle ut dette punktet, se vurderingsmomenter for prinsippet om riktighet i Veileder til IP, PLM og DPIA]* |
| Lagringsbegrensning  (GDPR art. 5 nr. 1 bokstav e) | *[For å fylle ut dette punktet, se vurderingsmomenter for prinsippet om lagringsbegrensning i Veileder til IP, PLM og DPIA]* |
| Integritet og konfidensialitet  (GDPR art. 5 nr. 1 bokstav f) | *[For å fylle ut dette punktet, se vurderingsmomenter for prinsippet om integritet og konfidensialitet i Veileder til IP, PLM og DPIA]* |
| Ansvarlighet  (GDPR art. 5 nr. 2) | *[For å fylle ut dette punktet, se vurderingsmomenter for prinsippet om ansvarlighet i Veileder til IP, PLM og DPIA]* |
| **Vurdering av personvernprinsippene samlet** | |
| Er alle personvernprinsippene *tilstrekkelig* ivaretatt? | Ja  Nei, angi hvilke personvernprinsipper som ikke er tilstrekkelig ivaretatt og begrunn hvorfor ikke |
|  | |

## 7D. Ivaretakelse av de registrertes rettigheter

|  |  |
| --- | --- |
|  | |
| *Beskriv hvordan alle de registrertes rettigheter i GDPR art. 12-22 blir ivaretatt eller legg inn lenke til informasjon om dette.* | |
| Rett til informasjon  (GDPR art. 12-14) | *[For å fylle ut dette punktet, se vurderingsmomenter for rett til informasjon i Veileder til IP, PLM og DPIA]* |
| Rett til innsyn  (GDPR art. 15) | *[For å fylle ut dette punktet, se vurderingsmomenter for rett til innsyn i Veileder til IP, PLM og DPIA]* |
| Rett til retting  (GDPR art. 16) | *[For å fylle ut dette punktet, se vurderingsmomenter for rett til retting i Veileder til IP, PLM og DPIA]* |
| Rett til sletting  (GDPR art. 17) | *[For å fylle ut dette punktet, se vurderingsmomenter for rett til sletting i Veileder til IP, PLM og DPIA]* |
| Rett til begrensning av behandling  (GDPR art. 18) | *[For å fylle ut dette punktet, se vurderingsmomenter for rett til begrensning i Veileder til IP, PLM og DPIA]* |
| Rett til dataportabilitet  (GDPR art. 20) | *[For å fylle ut dette punktet, se vurderingsmomenter for rett til dataportabilitet i Veileder til IP, PLM og DPIA]* |
| Rett til å protestere  (GDPR art. 21) | *[For å fylle ut dette punktet, se vurderingsmomenter for rett til å protestere i Veileder til IP, PLM og DPIA]* |
| Rett til å ikke være gjenstand for automatiserte individuelle avgjørelser, herunder profilering  (GDPR art. 22) | *[For å fylle ut dette punktet, se vurderingsmomenter for rett til* å ikke være gjenstand for automatiserte individuelle avgjørelser *i Veileder til IP, PLM og DPIA]* |
| **Vurdering av rettighetene samlet** | |
| Er alle rettighetene *tilstrekkelig* ivaretatt? | Ja  Nei, angi hvilke rettigheter som ikke er tilstrekkelig ivaretatt og begrunn hvorfor ikke |
|  | |

## 7E. Ivaretakelse av de registrertes friheter

|  |  |
| --- | --- |
|  | |
| *Beskriv hvordan alle de registrertes friheter etter blant annet Den europeiske menneskerettskonvensjonen (EMK) blir ivaretatt (hvis relevant) eller legg inn lenke til informasjon om dette.* | |
| Rett til respekt for privatliv og familieliv, hjem og kommunikasjon | *[For å fylle ut dette punktet, se vurderingsmomenter for rett til respekt for privatliv og familieliv, hjem og kommunikasjon i Veileder til IP, PLM og DPIA]* |
| Rett til ikke å bli diskriminert | *[For å fylle ut dette punktet, se vurderingsmomenter for rett til ikke å bli diskriminert i Veileder til IP, PLM og DPIA]* |
| Ytringsfrihet | *[For å fylle ut dette punktet, se vurderingsmomenter for ytringsfrihet i Veileder til IP, PLM og DPIA]* |
| Tanke-, tros- og religionsfrihet | *[For å fylle ut dette punktet, se vurderingsmomenter for tanke-, tros- og religionsfrihet i Veileder til IP, PLM og DPIA]* |
| **Vurdering av frihetene samlet** | |
| Er alle frihetene *tilstrekkelig* ivaretatt? | Ja  Nei, angi hvilke friheter som ikke er tilstrekkelig ivaretatt og begrunn hvorfor ikke |
|  | |

## 

## 7F. Databehandlere

*Denne delen besvares kun når det benyttes databehandlere.*

|  |  |
| --- | --- |
|  | |
| Hvem er databehandler? Ved flere databehandlere, skriv kun hoveddatabehandlere. |  |
| Brukes det underdatabehandlere? | Nei  Ja, angi hvem |
|  | |
| Er det inngått nødvendige databehandleravtaler i tråd med kravene i GDPR art. 28 nr. 3? | Ja  Nei, begrunn under |
|  | |
| Ved felles behandlingsansvar, er det inngått ordning eller avtale som regulerer forholdet til databehandlere? | Ja  Nei, begrunn under |
|  | |
| Er det stilt krav til databehandler, utover databehandleravtaler, om ivaretakelse av personvern og informasjonssikkerhet, f. eks. i samarbeidsavtale, kravspesifikasjon e.l.? | Nei  Ja, angi relevante dokumenter |
|  | |

# Risiko og tiltak

*Risikoene knyttet til ivaretakelse av personvern til den registrerte (personvernrisiko) omfatter risikoer for:*

* *brudd på personopplysningssikkerhet (personopplysningssikkerhetsrisiko)*
* *manglende oppfyllelse av prinsippene i GDPR art. 5 (personvernprinsipprisiko)*
* *manglende oppfyllelse av den registrertes rettigheter GDPR art. 12-22 (rettighetsrisiko)*
* *manglende oppfyllelse av grunnleggende friheter (frihetsrisiko)*

*Disse risikoene kan overlappe hverandre.*

*Spørsmålene i dette kapittelet sikrer at alle risikoer ved behandling av personopplysninger blir vurdert konkret og samlet.*

## 8A. Personopplysningssikkerhetsrisiko

*Behandlingsansvarlig skal vurdere personopplysningssikkerhetsrisiko etter GDPR art. 5 nr. 1 bokstav f, art. 24 og art. 32. dvs. krav til konfidensialitet, integritet, tilgjengelighet og robusthet. Vurdering av personopplysningssikkerhetsrisiko er også en del av risiko- og sårbarhetsanalyse (ROS).*

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| *Hvis ROS er gjennomført, legg ved ROS og fyll ut tabellen nedenfor med resultater fra ROS på tidspunkt for gjennomføring av denne vurderingen:* | | | |
| **Risk-ID** | **Uønsket hendelse** | | **Restrisiko (etter planlagte tiltak)** |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
| Oppsummert: Er alle identifiserte risikoer knyttet til personopplysningene håndtert, inkludert fastsettelse av tidsfrister og ansvarlige for gjennomføring av tiltakene? | | Ja  Nei, beskriv under | |
|  | | | |

|  |  |
| --- | --- |
|  | |
| Hvis ROS ikke er gjennomført, beskriv risiko, risikoens art, alvorlighetsgrad, samt planlagte tiltak for å håndtere risikoene og eventuelt legg ved en kort risikoanalyse: | |
|  | |
| Oppsummert: Er alle identifiserte risikoer knyttet til personopplysningene håndtert inkludert fastsettelse av tidsfrister og ansvarlige for gjennomføring av tiltakene? | Ja  Nei, beskriv under |
|  | |

## 8B. Annen personvernrisiko

*I denne delen vurderes risiko utover personopplysningssikkerhetsrisiko, dvs. risikoer knyttet til ivaretakelse av personvernprinsippene (personvernprinsipprisiko), de registrertes rettigheter (rettighetsrisiko) og de registrertes friheter (frihetsrisiko).*

|  |  |
| --- | --- |
|  | |
| Beskriv risiko, risikoens art, alvorlighetsgrad, samt planlagte tiltak for å håndtere risikoene og eventuelt legg ved en kort risikoanalyse: | |
|  | |
| Oppsummert: Er alle identifiserte risikoer knyttet til personvernprinsippene, de registrertes rettigheter og friheter håndtert og akseptable? | Ja  Nei |
| Er det noen restrisiko etter alle planlagte tiltak? | Ja  Nei |
| Beskriv restrisiko som virksomheten ikke kan ta ned etter ytterligere tiltak: | |
|  | |

# Involvering, risikoaksept og godkjenning

|  |  |
| --- | --- |
|  | |
| Er det behov for å gjennomføre en DPIA på bakgrunn av risikoene (inkl. restrisiko) og planlagte tiltak? | Ja, DPIA må gjennomføres  Nei |
| 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] |
| Risiko og restrisiko er akseptert av | [Navn] og [dato] |
| Godkjenning fra behandlingsansvarlig | [Navn] og [godkjenningsdato] |
| Godkjenning fra andre aktuelle roller f. eks. systemeier/løsningseier/prosjekteier (risikoeier) | [Navn] og [godkjenningsdato] |

# Vedlegg X

# PLM risikoanalyse: personvernprinsipper, rettigheter og friheter

| ID | Områder | Uønsket hendelse | Berørte | Årsak (utløsningskilde) | Konsekvens | Sann-synlighet | Risiko FØR tiltak | | | Tiltak | Antatt konsekvens etter tiltak | Antatt sann-synlighet etter tiltak | Risiko etter tiltak | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  | **Risiko knyttet til Personvernprinsippene:** |  | | | | | | | | | | | | | |
|  | Lovlighet herunder behandlingsgrunnlag |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Rettferdighet |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Åpenhet og forutsigbarhet |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Formålsbegrensninger |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Dataminimering |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Riktighet |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Lagringsbegrensninger |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Ansvarlighet |  |  |  |  |  |  | | |  |  |  |  | | |
|  | **Risiko knyttet til den registrertes rettigheter** |  | | | | | | | | | | | | | |
|  | Informasjon |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Innsyn |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Sletting |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Retting |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Begrensning av behandling (hvis relevant) |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Dataportabilitet (hvis relevant) |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Innsigelse (hvis relevant) |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Profilering/automatiserte avgjørelser (hvis relevant) |  |  |  |  |  |  | | |  |  |  |  | | |
|  | **Risiko knyttet til den registrertes friheter** |  | | | | | | | | | | | | | |
|  | Privatliv, familieliv, hjem og kommunikasjon |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Likebehandling |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Ytringsfrihet |  |  |  |  |  |  | | |  |  |  |  | | |
|  | Tanke-, tros- og religionsfrihet |  |  |  |  |  |  | | |  |  |  |  | | |
|  |  |  |  |  |  |  |  | | |  |  |  |  | | |