

**[Virksomhet]**

[Tittel på løsning/systemer/endringer/]

Dato for vurdering: [xx.xx.xxxx]

Mal: april 2022

Personvernkonsekvensvurdering ved høy risiko – DPIA

**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.

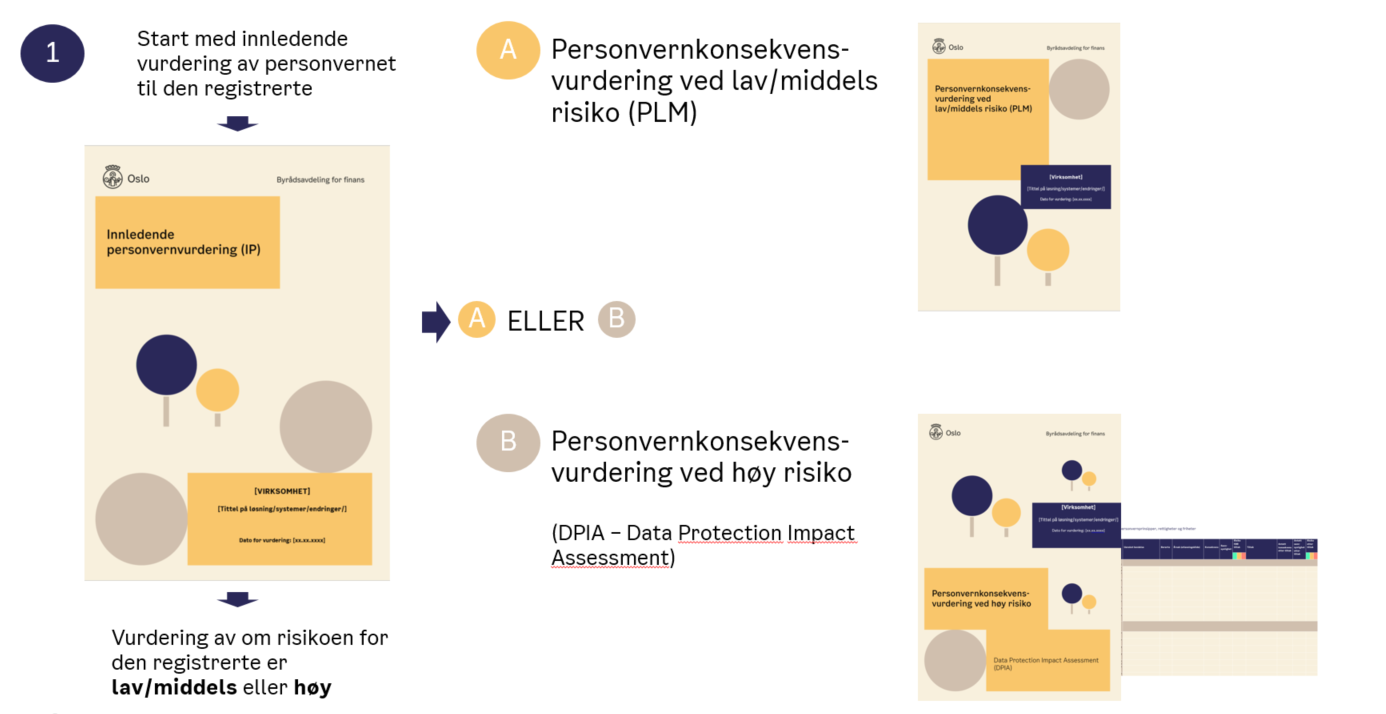
På bakgrunn av konklusjonen i *Innledende personvernvurdering (IP)* skal virksomheten gjennomføre enten *Personvernkonsekvensvurdering ved lav/middels risiko (PLM)* eller *Personvernkonsekvensvurdering ved høy risiko, DPIA.*

Hensikten med DPIA 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. DPIA vil også bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastsette risikoreduserende tiltak.

Spørsmålene i DPIA 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 DPIA 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. DPIA 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 6](#_Toc105073035)

[2. Grunnleggende informasjon om de registrerte 7](#_Toc105073036)

[3. Grunnleggende informasjon om personopplysninger 8](#_Toc105073037)

[4. Behandlingens art, omfang og kontekst 9](#_Toc105073038)

[4A. Beskrivelse av behandlingen 9](#_Toc105073039)

[4B. Behandlingens art 9](#_Toc105073040)

[4C. Behandlingens omfang 15](#_Toc105073041)

[4D. Behandlingens kontekst 16](#_Toc105073042)

[4E. Overføring til utlandet 18](#_Toc105073043)

[5. Behandlingens formål og begrunnelse 19](#_Toc105073044)

[5A. Formål for førstegangsbehandling 20](#_Toc105073045)

[5B. Formål ved viderebehandling 20](#_Toc105073046)

[5C. Begrunnelse for formålet 21](#_Toc105073047)

[6. Behandlingens lovlighet 21](#_Toc105073048)

[6A. Behandlingsgrunnlag 21](#_Toc105073049)

[6B. Samtykke 23](#_Toc105073050)

[7. Behandlingens nødvendighet og proporsjonalitet 24](#_Toc105073051)

[7A. Nødvendighetsvurdering 24](#_Toc105073052)

[7B. Proporsjonalitetsvurdering 24](#_Toc105073053)

[7C. Ivaretakelse av personvernprinsippene 25](#_Toc105073054)

[7D. Ivaretakelse av de registrertes rettigheter 26](#_Toc105073055)

[7E. Ivaretakelse av de registrertes friheter 28](#_Toc105073056)

[7F. Databehandlere 29](#_Toc105073057)

[7G. Samlet vurdering 29](#_Toc105073058)

[8. Risiko og tiltak 30](#_Toc105073059)

[8A. Personopplysningssikkerhetsrisiko 30](#_Toc105073060)

[8B. Personvernprinsipprisiko 31](#_Toc105073061)

[8C. Rettighetsrisiko 32](#_Toc105073062)

[8D. Frihetsrisiko 33](#_Toc105073063)

[8E. Oppsummering av restrisiko 34](#_Toc105073064)

[9. Involvering, risikoaksept og godkjenning 34](#_Toc105073065)

[9A. Involvering 34](#_Toc105073066)

[9B. Risikoaksept 36](#_Toc105073067)

[9C. Godkjenning 36](#_Toc105073068)

**Vedlegg X**: Risikoanalyse for personvernrisiko

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

Spørsmålene i DPIA 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] | |
| Er det gjennomført andre personvernvurderinger eller DPIA som har betydning for den planlagte behandling? | Nei  Ja, angi  Hvis mulig, legg ved relevante personvernvurderinger eller DPIA. | |
| Ved felles behandlingsansvar, er det inngått en ordning eller avtale om felles behandlingsansvar (GDPR 26 nr. 1)? | Nei  Ja, angi | |
| Finnes det andre avtaler, dokumenter, ordninger ol. som kan ha betydning for DPIA? | Nei  Ja, angi | |

# Grunnleggende informasjon om de registrerte

Spørsmålet i DPIA 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 DPIA 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 DPIA 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 eller trykk her for å skrive inn tekst. |
| **Innsamling** | |
| 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. |
| Kan måten personopplysningene samles inn på, anses som inngripende for den registrerte (for eksempel ved hjelp av kamera- eller lydopptak, fingeravtrykk, biometri og geolokasjon)? | Nei  Ja, beskriv under |
| Er alle personopplysningene som samles inn nødvendig for å oppnå formålet med behandlingen? | Ja  Nei, beskriv under  Klikk her for å skrive inn tekst. |
| **Lagring** | |
| Hvordan skal personopplysningene lagres? | Klikk her for å skrive inn tekst. |
| Hvor skal personopplysningene lagres? | Klikk her for å skrive inn tekst. |
| Hvor lenge skal personopplysningene lagres? | Antall dager/måneder/år eller annen tidfesting |
| Hvilke kriterier brukes for å avgjøre lagringstid? |  |
| **Retting** | |
| Skal personopplysningene kunne rettes? | Nei  Ja  Klikk her for å skrive inn tekst. |
| Finnes det rettsgrunnlag i lov eller forskrift som gir grunnlag for å nekte retting? | Nei  Ja, med grunnlag i:  Klikk her for å skrive inn tekst. |
| Hvordan skal retting skje? | Den registrerte kan rette selv  Den registrerte må kontakte virksomheten |
| Er det laget rutiner for retting? | Ja  Nei |
| **Sletting** | |
| Skal personopplysningene kunne slettes? | Ja  Nei |
| Når skal personopplysningene slettes? | Antall dager/måneder/år eller annen tidfesting |
| Hvordan skal sletting skje? | Den registrerte kan slette selv  Den registrerte må kontakte virksomheten |
| Er det laget rutiner for sletting? | Ja  Nei |
| **Tilgang, deling, utlevering og tilgjengeliggjøring** | |
| 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. |
| Er det vurdert at virksomheten har behandlingsgrunnlag for deling, utlevering eller tilgjengeliggjøring av personopplysninger for virksomheter eller personer utenfor egen virksomhet i eller utenfor Oslo kommune?  *[Deling, utlevering eller tilgjengeliggjøring av personopplysninger kan føre til endret risiko for personvernet og at behandlingen er utenfor den registrertes forventninger til behandlingen av personopplysninger. Det må sikres at deling, utlevering eller tilgjengeliggjøring er i tråd med formålene og at behandlingsgrunnlaget tillater dette. Husk at selv om virksomheten er behandlingsansvarlig for flere datasett i flere løsninger betyr det ikke at dataene kan deles, utleveres eller tilgjengeliggjøres fritt.]* | Nei  Ja, angi behandlingsgrunnlag |
| Hvis behandlingsgrunnlaget ikke tillater deling, utlevering eller tilgjengeliggjøring av personopplysninger, er det inngått avtaler med mottakerne av data/personopplysninger? | Nei  Ja, angi med hvem og dato |
| **Sammenstilling** | |
| Skal personopplysningene sammenstilles? | Nei  Ja, sammenstilles:  Fra én datakilde i eller utenfor Oslo kommune  Fra flere datakilder innenfor Oslo kommune  Fra flere datakilder utenfor Oslo kommune |
| Er det vurdert at sammenstillingen er innenfor de aktuelle datakildenes formål? | Nei, begrunn under  Ja, beskriv under |
|  | | |
| Er det vurdert at virksomheten har behandlingsgrunnlag for sammenstilling av personopplysninger?  *[Sammenstilling av personopplysninger kan føre til endret risiko for personvernet og at behandlingen er utenfor den registrertes forventninger til behandlingen av personopplysninger. Det må sikres at sammenstillingen er i tråd med formålene og at behandlingsgrunnlagene for de aktuelle datakildene tillater sammenstilling. Husk at selv om virksomheten er behandlingsansvarlig for flere datasett i flere løsninger betyr det ikke at dataene kan sammenstilles fritt.]* | Nei  Ja, angi behandlingsgrunnlag |
| Hvis behandlingsgrunnlagene ikke tillater sammenstilling av personopplysninger, er det inngått avtaler med behandlingsansvarlig for datakildene? | Nei  Ja, angi med hvem og dato |

## 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. |
| Hvor ofte skal innsamlingen av personopplysningene skje? | Samles inn én gang  Samles inn periodisk  Samles inn kontinuerlig |
| Hvor ofte skal personopplysningene behandles? | Engangsbehandling  Periodisk behandling  Kontinuerlig behandling |
| I hvilket geografisk område befinner de registrerte seg? | Klikk her for å skrive inn tekst. |
| Beskriv andre momenter som har betydning for behandlingens omfang (f. eks.om det behandles flere kategorier av personopplysninger, volum av personopplysninger, geografisk utbredelse osv.): | |
|  | |

## 4D. Behandlingens kontekst

|  |  |
| --- | --- |
|  | |
| Hvilken relasjon har virksomheten til de registrerte? | Oslo kommune som myndighet (inkl. når Oslo kommune opptrer som tilskuddsyter eller politisk myndighet) og innbyggere som privatperson eller innbyggere i næring/som profesjonsutøver f.eks. regnskapsfører, revisor osv.  Oslo kommune som leverandør/tjenestetilbyder og innbyggere/kunde/brukere  Oslo kommune som arbeidsgiver og arbeidstaker  Oslo kommune som løsningseier/systemeier/dataeier og innbyggere (f. eks. ifbm. forskningsprosjekt)  Oslo kommune som eier/forvalter/utvikler og privatperson eller profesjonelle aktører  Helse-, omsorg- og sosialtjenestetilbyder (inkl. skolehelsetjeneste, tannhelsetjeneste, helsestasjon mv.) og pasienter/brukere/pårørende  Skole og elever eller studenter  Barnehage og barnehagebarn  Ombudsrolle og brukere/innbyggere  Annet:  Klikk eller trykk her for å skrive inn tekst. |
| Hvilken grad av kontroll har de registrerte over sine personopplysninger? *[Kryss av]* | Stor kontroll og valgfrihet  Middels kontroll og valgfrihet  Ingen kontroll og valgfrihet |
| Vil de registrerte forvente at personopplysninger om dem brukes på den måten som i den planlagte behandlingen? | 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 |
|  | |
| Innebærer behandlingen på noen måte en ny eller endret prosess? | Nei  Ja, beskriv under |
|  | |
| Er det tidligere avdekket risikoer/bekymringer og sikkerhetsbrudd eller finnes det offentlig kjente problemer med tilsvarende behandling (f. eks. problemer med bruken av teknologi)? | Nei  Ja, beskriv under |
|  | |
| Brukes teknologi som er vanlig og nåværende standard for denne typen behandling? | Ja  Nei, begrunn under |
|  | |
| Beskriv andre momenter som kan påvirke rimelige forventninger fra de registrerte eller påvirke konsekvenser av behandling 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 overføring av personopplysninger til land innenfor EU/EØS? | Nei  Ja  Angi til hvilket land |
| Er det planlagt overføring av personopplysninger til land utenfor EU/EØS (tredjeland) som er godkjent av EU-kommisjonen? | Nei  Ja  Angi til hvilket land |
| **Overføring av personopplysningene til land utenfor EU/EØS (tredjeland) som ikke er godkjent av EU-kommisjonen** | |
| Er det planlagt overføring av personopplysninger til land utenfor EU/EØS (tredjeland) som ikke er godkjent av EU-kommisjonen? | Nei  Ja  Angi til hvilket land |
| Hvilket overføringsgrunnlag er benyttet for å sikre lovlig overføring?  *[For beskrivelse av overføringsgrunnlag, se Veileder til IP, PLM og DPIA]* | Standard personvernbestemmelser vedtatt av tilsynsmyndighet og godkjent av EU-kommisjonen  Bindende virksomhetsregler  Standard personvernbestemmelser vedtatt av EU-kommisjonen  Annet, beskriv under |
|  | |
| Hvilke ytterligere tiltak iverksettes utover lovlig overføringsgrunnlag? |  |

# Behandlingens formål og begrunnelse

Spørsmålene i DPIA 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. |
|  |
| Ved flere behandlingsaktiviteter med ulike formål, skal formålet for hver enkel behandlingsaktivitet detaljeres, listes opp eller evt. grupperes her. |
|  |

## 5B. Formål ved viderebehandling

|  |  |
| --- | --- |
|  | |
| Hva er formålet med viderebehandling av personopplysninger (nytt formål)? |  |
| Hva er det opprinnelige formålet med behandlingen? |  |
| Er det gjennomført en forenlighetstest mellom det nye formålet og det opprinnelige formålet?  *[For hvordan gjennomføre forenlighetstest, se Veileder om behandlingsgrunnlag]* | Ja  Nei, begrunn under |
|  | |
| Er det forenlighet mellom det nye formålet og det opprinnelige formålet? | Nei  Ja, beskriv under |
|  | |

## 5C. Begrunnelse for formålet

|  |  |
| --- | --- |
|  | |
| Hva ønsker virksomheten å oppnå med behandlingen (ønsket effekt)? |  |
| Hva er fordeler med behandlingen? |  |
| Ut fra hva virksomheten ønsker å oppnå med behandlingen (ønsket effekt) og fordeler og ulemper med behandlingen, er det fastsatte formålet forholdsmessig? |  |

# 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): | |
|  | |
| Begrunn kort hvorfor det spesifikke behandlingsgrunnlaget er valgt: | |
|  | |

## 6B. Samtykke

Denne delen skal kun besvares 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 |
|  | |
| Finnes det andre eller mindre inngripende måter å behandle personopplysningene på? | Nei  Ja, beskriv under |
|  | |
| Beskriv hvorfor den andre eller mindre inngripende måten ikke brukes: | |
|  | |

## 7B. Proporsjonalitetsvurdering

|  |  |
| --- | --- |
|  | |
| Er det et rimelig forhold mellom inngrepet som gjøres i personvernet og de fordelene som oppnås ved behandlingen? | Nei  Ja, beskriv under |
|  | |
| Beskriv hvorfor valgt behandling anses som passende og rimelig for å oppnå formålet: | |
|  | |

## 7C. Ivaretakelse av personvernprinsippene

|  |  |
| --- | --- |
|  | |
| *Beskriv nedenfor 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 |
|  | |
| Finnes det ytterligere mulighet til å forbedre gjennomføring av personvernprinsippene? | Nei  Ja, beskriv og begrunn under hvorfor mulighetene ikke vil bli valgt |
|  | |

## 7D. Ivaretakelse av de registrertes rettigheter

|  |  |
| --- | --- |
|  | |
| *Beskriv nedenfor hvordan alle de registrertes rettigheter i GDPR art. 12-22 ivaretas 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 under hvorfor ikke |
|  | |
| Finnes det ytterligere mulighet til å forbedre ivaretakelsen av de registrertes rettigheter? | Nei  Ja, beskriv og begrunn under hvorfor mulighetene ikke vil bli valgt |
|  | |

## 7E. Ivaretakelse av de registrertes friheter

|  |  |
| --- | --- |
|  | |
| *Beskriv nedenfor hvordan alle de registrertes friheter etter blant annet Den europeiske menneskerettskonvensjonen (EMK) ivaretas (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 under hvorfor ikke |
|  | |
| Finnes det ytterligere mulighet til å forbedre ivaretakelsen av de registrertes friheter? | Nei  Ja, beskriv og begrunn under hvorfor mulighetene ikke vil bli valgt |
|  | |

## 

## 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 |
|  | |

## 7G. Samlet vurdering

|  |  |
| --- | --- |
|  | |
| *I denne delen gjøres det en samlet vurdering av svarene del A-F* | |
| Basert på svarene i del A-F, er behandlingen nødvendig? | Ja  Nei, begrunn under hvorfor ikke |
|  | |
| Basert på svarene i del A-F, kan fordelene med behandlingen oppveies av personvernulempene? | Ja  Nei, begrunn under hvorfor ikke |
|  | |

# 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 kapitlet 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).*

*Dersom det allerede er gjennomført en ROS, bør ROS vedlegges og fyll ut tabellen nedenfor. Dersom det ikke er gjennomført en ROS ved oppstart av DPIA, skal ROS gjennomføres parallelt med DPIA. [Se på mal og veileder for ROS].*

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| Er det gjennomført en ROS? | | Ja  Nei | |
| Fyll ut tabellen nedenfor med resultater fra ROS på tidspunkt for gjennomføring av DPIA: | | | |
| **Risk-ID** | **Uønsket hendelse** | | **Restrisiko (etter planlagte tiltak)** |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
| Basert på resultatet av ROS, er krav til konfidensialitet, integritet, tilgjengelighet og robusthet ved behandling av personopplysningene *tilstrekkelig* ivaretatt? | | Ja  Nei, beskriv under | |
|  | | | |
| Oppsummert: Er alle identifiserte risikoer knyttet til personopplysningene håndtert (inkludert fastsettelse av tidsfrister og ansvarlige for gjennomføring av tiltakene) og akseptable? | | Ja  Nei, beskriv under | |
|  | | | |

## 8B. Personvernprinsipprisiko

*For å fylle ut denne delen, må det først gjennomføres en risikoanalyse knyttet til personvernprinsippene i vedlegg X.*

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| Er risikoanalyse knyttet til personvernprinsippene i vedlegg X gjennomført? | | Ja  Nei | |
| Fyll ut tabellen nedenfor med resultater fra risikoanalyse: | | | |
| **Risk-ID** | **Uønsket hendelse** | | **Restrisiko (etter tiltak)** |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
| Basert på resultatet av risikoanalyse, er alle personvernprinsippene *tilstrekkelig* ivaretatt ved behandling av personopplysninger? | | Ja  Nei, beskriv under | |
|  | | | |
| Oppsummert: Er alle identifiserte risikoer knyttet til personvernprinsippene håndtert og akseptable? | | Ja  Nei, beskriv under | |
|  | | | |

## 8C. Rettighetsrisiko

For å fylle ut denne delen, må det først gjennomføres en risikoanalyse knyttet til den registrertes rettigheter i vedlegg X.

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| Er risikoanalyse knyttet til den registrertes rettigheter i vedlegg X gjennomført? | | Ja  Nei | |
| Fyll ut tabellen nedenfor med resultater fra risikoanalyse: | | | |
| **Risk-ID** | **Uønsket hendelse** | | **Restrisiko (etter tiltak)** |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
| Basert på resultatet av risikoanalyse, er alle den registrertes rettigheter *tilstrekkelig* ivaretatt ved behandling av personopplysninger? | | Ja  Nei, beskriv under | |
|  | | | |
| Oppsummert: er alle identifiserte risikoer knyttet til den registrertes rettigheter håndtert og akseptable? | | Ja  Nei, beskriv under | |
|  | | | |

## 8D. Frihetsrisiko

For å fylle ut denne delen, må det først gjennomføres en risikoanalyse knyttet til den registrertes rettigheter i vedlegg X.

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| Er risikoanalyse knyttet til den registrertes friheter i vedlegg X gjennomført? | | Ja  Nei | |
| Fyll ut tabellen nedenfor med resultater fra risikoanalyse: | | | |
| **Risk-ID** | **Uønsket hendelse** | | **Restrisiko (etter tiltak)** |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
| Basert på resultatet av risikoanalyse, er alle den registrertes friheter *tilstrekkelig* ivaretatt ved behandling av personopplysninger? | | Ja  Nei, beskriv under | |
|  | | | |
| Oppsummert: er alle identifiserte risikoer knyttet til den registrertes friheter håndtert og akseptable? | | Ja  Nei, beskriv under | |
|  | | | |

## 8E. Oppsummering av restrisiko

|  |  |
| --- | --- |
|  | |
| Er det restrisiko som virksomheten ikke kan ta ned etter ytterligere tiltak? | Ja  Nei |
| Beskriv restrisiko som virksomheten ikke kan ta ned etter ytterligere tiltak: | |
|  | |

# Involvering, risikoaksept og godkjenning

## 9A. Involvering

|  |  |
| --- | --- |
|  | |
| **De registrerte/bruker- og interesseorganisasjoner** | |
| Har de registrerte eller bruker- og interesseorganisasjoner vært involvert? | Nei  Ja, skriv når og hvordan: |
|  | |
| **Databehandlere** | |
| Har det vært behov for å involvere databehandler? Legg eventuelt ved relevant dokumentasjon. | Ja, [navn, rolle/funksjon]  Nei, begrunn under |
|  | |
| **Fagressurser**  *Ved behov kan det innhentes råd/veiledning fra fagpersoner/eksperter, FIN/ISI og PKO/ISK på byrådavdelingsnivå med ansvar for sektoren* | |
| Har det vært behov for å involvere eksperter eller andre fagpersoner internt i Oslo kommune (f. eks. informasjonssikkerhet- eller IT-personell, jurister mv.)? | Nei  Ja,  [navn, rolle/funksjon, virksomhetsnavn] |
|  | |
| Er det innhentet råd/veiledning fra sentralt fagmiljø for personvern og informasjonssikkerhet i Oslo kommune (FIN/ISI)?  *[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.]* | Nei  Ja, skriv [navn, rolle] |
|  | |
| Er det innhentet råd/veiledning fra ansvarlige byrådsavdelinger? | Nei  Ja, skriv [navn, navn på byrådsavdeling] |
|  | |
| Har det vært behov for å innhente innspill eller involvere eksperter eller andre fagpersoner utenfor Oslo kommune? | Nei  Ja, skriv [virksomhetsnavn, kontaktpersons navn, rolle/funksjon] |
|  | |
| **Personvernombudet**  *Etter GDPR art. 35 nr. 2 skal behandlingsansvarlig rådføre seg med Personvernombudet i forbindelse med utførelsen av DPIA. Dersom Personvernombudet har gitt råd eller anbefalinger i eget dokument, skal dette vedlegges.* | |
| Er det innhentet råd fra Personvernombudet?  *[Personvernombudet skal ikke gjennomføre denne vurderingen, og Personvernombudets involvering er kun ment som veiledning til konkrete spørsmål og kan ikke anses som en godkjenning av vurderingen.]* | Nei, begrunn:  Ja, skriv når |
|  | |
| Skriv en oppsummering av Personvernombudets anbefalinger her: | |
|  | |
|  | |

## 9B. Risikoaksept

|  |  |
| --- | --- |
|  | |
| Risiko og restrisiko er akseptert av | [Navn] og [dato] |
| Hvis Personvernombudet har frarådet fortsatt behandling av personopplysninger og virksomhetsleder beslutter at behandlingen allikevel iverksettes, skriv begrunnelse her. Dersom begrunnelse gis i eget dokument, skal dette vedlegges og begrunnelsen kort oppsummeres her. | |
|  | |
| På bakgrunn av restrisiko, er det behov for forhåndsdrøfting med Datatilsynet?  GDPR art. 36 nr. 1 | Ja  Nei |
| Hvis virksomhetsleder bestemmer at Datatilsynet ikke skal konsulteres, skriv begrunnelse her. Dersom begrunnelse gis i eget dokument, skal dette vedlegges og begrunnelsen kort oppsummeres her. | |
|  | |

## 9C. Godkjenning

*Navn og dato i denne tabellen skrives kun når DPIA er sluttført og godkjent.*

|  |  |
| --- | --- |
|  | |
| Vurderingen er sluttført 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

# DPIA 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 |  |  |  |  |  |  | | |  |  |  |  | | |
|  |  |  |  |  |  |  |  | | |  |  |  |  | | |