**Mal fra nettverk for personvernombud i fylkeskommuner:**

**Vurdering av personvernkonsekvenser (DPIA)**

**Om personvernkonsekvensvurderingen**

Vurdering av personvernkonsekvenser er en prosess som skal sikre enkeltpersoners rettigheter og friheter der behandlingen av personopplysninger kan medføre høy risiko.

Vurderingen av personvernkonsekvenser skal gjøres før behandlingen av personopplysninger starter opp. Det kan også være endringer i pågående behandlingsaktiviteter som krever ny eller oppdatert vurdering.

En vurdering av personvernkonsekvensene skal den minst inneholde:

* Systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene
* Vurdering av om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålene
* Vurdering av risikoene for de registrertes friheter og rettigheter
* Beskrivelse av de planlagte tiltakene for å håndtere risikoene

Den behandlingsansvarlige må ta stilling til om den planlagte behandlingsaktiviteten krever en vurdering av personvernkonsekvenser.

Basert på vurderingene og anbefalingene, samt personvernombudets og de registrertes uttalelse, skal den behandlingsansvarlige foreta en beslutning om videre behandling:

*Er behandlingen nødvendig og rimelig, kan vi påvise at forordningen overholdes og kan de registrertes rettigheter og friheter ivaretas?*

Om dette ikke kan ivaretas, så kan behandlingen av personopplysninger ikke startes eller opprettholdes.

Se artikkel 35 i personopplysningsloven for nærmere beskrivelse av kriterier og vurdering av personvernkonsekvenser.

**Om malen**

Malen starter med identifisering av roller og ansvar i kapittel 2 og avsluttes med å oppsummere arbeidsgruppas vurderinger og anbefalinger i kapittel 1. Vurdering av behov for gjennomføring av personvernkonsekvensvurderingen forutsettes utført før arbeidet starter. Dette inngår ikke i malen.

Malen er veiledende, den kan tilpasses etter egne behov og spørsmål besvares i den grad de er relevante for vurderingen. Det kan også være at spørsmål bør legges til for å belyse behandlingsaktiviteten i tilstrekkelig grad.

Se eget dokument *Veiledning til vurdering av personvernkonsekvenser med ordliste* for praktisk hjelp for gjennomføring av vurderingen.

Dokumenter:

* *Vurdering av personvernkonsekvenser (DPIA)*
* *Veiledning til vurdering av personvernkonsekvenser med ordliste*
* *Behandlingsansvarliges vurdering og beslutning*

Malen og tilhørende dokumenter kan ikke benyttes til kommersielle formål uten tillatelse fra personvernombudene i fylkeskommunene.



*Illustrasjon av prosess for vurdering av personvernkonsekvenser (DPIA).*

Innhold

[1. ARBEIDSGRUPPAS VURDERINGER OG ANBEFALING 5](#_Toc123729755)

[Arbeidsgruppas anbefaling 5](#_Toc123729756)

[Arbeidsgruppas vurderinger 5](#_Toc123729757)

[Nødvendighet og rimelighet 5](#_Toc123729758)

[Vurdering av risiko 6](#_Toc123729759)

[Vurdering av tiltak 6](#_Toc123729760)

[Vurdering av usikkerhet 6](#_Toc123729761)

[Identifiserte risikoer og tiltak 6](#_Toc123729762)

[Personvernombud og registrertes uttalelse 6](#_Toc123729763)

[Personvernombudets uttalelse 6](#_Toc123729764)

[Registrertes uttalelse 6](#_Toc123729765)

[2. ORGANISERING - roller og ansvar for gjennomføringen 8](#_Toc123729766)

[3. BESKRIVELSE AV BEHANDLINGSAKTIVITETEN 9](#_Toc123729767)

[Formål 9](#_Toc123729768)

[Overordnet beskrivelse av behandlingsaktiviteten 9](#_Toc123729769)

[Virksomheter med ansvar og deres rolle i behandlingsaktiviteten (behandlingsansvar, databehandlere og ev. felles behandlingsansvar) 9](#_Toc123729770)

[Hvilke personopplysninger behandles og hvem behandles det personopplysninger om? 10](#_Toc123729771)

[Hvem/hvor kommer personopplysningene fra? 10](#_Toc123729772)

[Oppdatering, endring og retting 10](#_Toc123729773)

[Sletting, destruksjon eller anonymisering 11](#_Toc123729774)

[Tilgang til personopplysningene 11](#_Toc123729775)

[Utlevering til tredjeparter – selvstendig behandlingsansvarlige 11](#_Toc123729776)

[Overføring til tredjeland (overføring eller tilgjengeliggjøring til land utenfor EU/EØS) 11](#_Toc123729777)

[Dataflyt og integreringer 11](#_Toc123729778)

[Sikring av personopplysningene (personopplysningssikkerhet) 11](#_Toc123729779)

[Lovlighet 12](#_Toc123729780)

[Behandlingsgrunnlag 12](#_Toc123729781)

[Beskriv behandlingsaktiviteten 12](#_Toc123729782)

[Besvarelse/utdypning 12](#_Toc123729783)

[Unntak for behandling av særlige kategorier personopplysninger 12](#_Toc123729784)

[Informasjon, åpenhet og håndtering av rettigheter 14](#_Toc123729785)

[Dokumentasjon - vedlegg 14](#_Toc123729786)

[4. VURDERING AV RISIKOER OG TILTAK 15](#_Toc123729787)

[PERSONVERNPRINSIPPENE 15](#_Toc123729788)

[Lovlighet 15](#_Toc123729789)

[Rettferdighet 16](#_Toc123729790)

[Åpenhet 17](#_Toc123729791)

[Formålsbegrensning 18](#_Toc123729792)

[Dataminimering 19](#_Toc123729793)

[Riktighet 20](#_Toc123729794)

[Lagringsbegrensning 21](#_Toc123729795)

[Integritet og konfidensialitet 22](#_Toc123729796)

[REGISTRERTES RETTIGHETER 23](#_Toc123729797)

[Oversikt over relevante rettigheter ifm. behandlingsaktiviteten 23](#_Toc123729798)

[Generell behandling av rettighetsforespørsler 23](#_Toc123729799)

[Rett til informasjon 24](#_Toc123729800)

[Rett til innsyn 25](#_Toc123729801)

[Rett til retting og sletting 26](#_Toc123729802)

[Rett til begrensning 27](#_Toc123729803)

[Rett til å protestere 27](#_Toc123729804)

[GRUNNLEGGENDE RETTIGHETER OG FRIHETER 28](#_Toc123729805)

[5. VURDERING AV NØDVENDIGHET OG RIMELIGHET 31](#_Toc123729806)

[Er behandlingsaktiviteten nødvendig? 31](#_Toc123729807)

[Hvor inngripende er behandlingsaktiviteten? 31](#_Toc123729808)

[Er behandlingsaktiviteten proporsjonal og rimelig? 32](#_Toc123729809)

[6. Referanser 32](#_Toc123729810)

[7. Vedlegg 33](#_Toc123729811)

# ARBEIDSGRUPPAS VURDERINGER OG ANBEFALING

Arbeidsgruppas vurderinger og anbefaling baseres på vurderingens øvrige deler og skrives til slutt.

Vurderingens formål og omfang

|  |
| --- |
| **Vurderingens formål og omfang** |
| Hvilken eller hvilke behandlinger, tjenester eller prosesser inngår i vurderingen? |
|   |
| Hva er bakgrunnen for vurderingen av personvernkonsekvensene?  |
|   |
| Er det gjort særskilte avgrensinger i vurderingen?  |
|   |
| Øvrige kommentarer  |
|    |

## Arbeidsgruppas anbefaling

Arbeidsgruppas anbefaling om igangsetting eller videre behandling av personopplysninger.

|  |
| --- |
| **Arbeidsgruppas anbefaling**  |
| **Behandlingsaktiviteten kan iverksettes eller videreføres uten ytterligere tiltak**Behandlingsaktiviteten kan iverksettes eller videreføres dersom det ikke er identifisert risikoer eller andre forhold som krever tiltak. Det kan likevel være tiltak som anbefales for bedre ivaretakelse av personvernet. | **Behandlingsaktiviteten kan iverksettes eller videreføres med påkrevde tiltak**Dersom påkrevde tiltak eller tiltak med tilsvarende effekt implementeres, kan behandlingsaktiviteten iverksettes eller videreføres. Anbefalte tiltak skal iverksettes der er hensiktsmessig. | **Behandlingsaktiviteten krever forhåndsvurdering**Viser vurderingen av personvernkonsekvenser at behandlingsaktiviteten vil medføre høy risiko også etter identifiserte tiltak, skal behandlingsansvarlig rådføre seg med Datatilsynet. | **Behandlingsaktiviteten bør ikke iverksettes eller videreføres**Vurderingen av nødvendighet og rimelighet og/eller risiko etter identifiserte tiltak, viser at behandlingsaktiviteten ikke bør iverksettes eller videreføres. |
| [ ]  | [ ]  | [ ]  | [ ]  |
| Angi arbeidsgruppas begrunnelse. |
|  |

## Arbeidsgruppas vurderinger

Arbeidsgruppas oppsummering av vurderingene som er gjennomført i påfølgende kapitler.

|  |
| --- |
| **Arbeidsgruppas vurderinger** |
| Nødvendighet og rimelighetEr behandlingsaktivitetene nødvendige og står de i rimelig forhold til formålene? |
|  |
| Vurdering av risikoEr det avdekket uakseptabel risiko med hensyn til personvernforordningens prinsipper, de registrertes personvernrettigheter eller for grunnleggende rettigheter og friheter. |
|  |
| Vurdering av tiltakVil gjennomføring av de identifiserte tiltakene føre til at risikoene vil være innenfor akseptabelt nivå? |
|  |
| Vurdering av usikkerhetForeligger usikkerhet knyttet til vurderingene som er viktig å merke seg? |
|  |

## Identifiserte risikoer og tiltak

Oppsummering av vesentlige risikoer samt nødvendige eller anbefalte tiltak. Nødvendige tiltak eller tiltak med tilsvarende effekt, skal gjennomføres før behandlingsaktiviteten starter. Anbefalte tiltak vil forbedre personvernet, men kan vurderes f.eks. i forhold til kostnadseffektivitet.

Risiko og tiltak hentes fra vurderingene i kapittel 4.

|  |
| --- |
| **Vesentlige risikoer hvor tiltak er vurdert som nødvendig eller anbefalt**  |
| Risiko ID | Risiko | Tiltaks ID | Beskrivelse av tiltak | Nødvendig eller anbefalt |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Personvernombud og registrertes uttalelse

Personvernombudets og registrertes uttalelse skal vektlegges i behandlingsansvarliges vurdering og konklusjoner. Dersom konkrete råd i personvernombudets uttalelse ikke følges, skal dette begrunnes i *Behandlingsansvarliges vurdering og beslutning.*

|  |
| --- |
| Personvernombudets uttalelse(Henvis til vedlegg om ønskelig) |
| Personvernombudets kommentar til rapporten og behandlingen, herunder om personvernombudet enig i arbeidsgruppas konklusjon. |
|  |

Dersom det er relevant, skal den behandlingsansvarlige innhente synspunkter på den planlagte behandlingen fra de registrerte eller deres representant/er.

|  |
| --- |
| Registrertes uttalelse (Henvis til vedlegg om ønskelig) |
| De registrertes uttalelse kan innhentes fra en eller flere representanter for de registrerte. Representantene bør legge vekt på om det er vesentlige risikoer som ikke er identifisert, om tiltakene er tilstrekkelige og om de anser behandlingen som nødvendig og rimelig.  |
|  |

#

# ORGANISERING - roller og ansvar for gjennomføringen

Avklaring av ansvar og roller er viktig ved gjennomføring av en personvernkonsekvensvurdering. Arbeidsgruppen bør settes i sammen slik at tverrfaglig kompetanse knyttet til behandlingsaktiviteten og personvern ivaretas.

Her er roller og ansvar fordelt i forhold til hvem som er hovedansvarlig for behandlingsaktiviteten som skal vurderes, hvem som skal utføre vurderingen herunder leder og deltagere i arbeidsgruppen, hvem som skal konsulteres og hvem som skal informeres om vurderingen. Tabellen er delvis utfylt og tilpasses etter behov.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Navn og tittel** | **Rolle i arbeidsgruppa** | **Hovedansvarlig for behandlingen** | **Utførende**  | **Konsulteres** | **Informeres** |
|  | Hovedansvarlig for personvern i behandlingsaktiviteten | **X** |  | **X** | **X** |
|  | Leder i arbeidsgruppe |  | **X** |  |  |
|  | Medlem i arbeidsgruppe |  | **X** |  |  |
|  | Medlem i arbeidsgruppe |  | **X** |  |  |
|  | Medlem i arbeidsgruppe |  | **X** |  |  |
|  | Personvernombud |  |  | **X** | **X** |
|  | Registrertes repr. |  |  | **X** |  |
|  | Øvrige |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# BESKRIVELSE AV BEHANDLINGSAKTIVITETEN

Beskrivelsen av behandlingsaktivitetene er et selvstendig krav i personvernforordningen og gir et deskriptivt grunnlag for den videre vurderingen.

Det kan være hensiktsmessig å legge ved ytterligere beskrivelser og dokumentasjon slik som vurderinger av lovlighet, beskrivelser av tekniske og organisatoriske tiltak, personvernerklæringer m.m.

Dersom behandlingen som vurderes er pågående og protokoll er utfylt kan deler av informasjonen hentes fra denne eller f.eks. fra inngått databehandleravtale.

|  |
| --- |
|  Formål |
| Hva er formålet med behandlingen? |
|  |
| Beskriv eventuelle underformål. Disse kan stå i sammenheng med prosesser som inngår i behandlingen.Et formål kan være å utvikle kompetanse hos ansatte. Underformål kan da være å kartlegge kompetanse og dokumentere at opplæring er gitt. |
|  |
| Hva skal behandlingen ivareta eller løse? Beskriv hvilke behov, nytte, hensyn og interesse hos behandlingsansvarlig som ligger bak formålet. |
|  |
| Er personopplysningene tenkt viderebehandlet til nye eller andre formål enn beskrevet over? F.eks. arkivformål, dokumentasjonsbehov, forskning, utvikling av tjenester mv. |
|  |

|  |
| --- |
| Overordnet beskrivelse av behandlingsaktiviteten |
| Gi en kort og overordnet beskrivelsen av behandlingen, dens prosesser og omfang. |
|  |
| Beskriv hvilke operasjoner som inngår i behandlingen. F.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring, |
|  |
| Hvilke grupper/aktører har en hovedrolle i selve innsamlingen og videre behandling av personopplysningene? |
|  |
| Hvilke IKT-systemer, applikasjoner eller tjenester eller tilsvarende inngår i behandlingsaktiviteten? |
|  |
| Dersom det er viktig for å forstå risikobildet herunder behov for konfidensialitet, beskriv relevant sammenheng behandlingsaktiviteten skjer i. Dette kan være fysiske, lokasjonsmessige, organisatoriske eller menneskelige forhold slik som Teams-møte hvor deltakerne sitter i private hjem eller hvor geolokasjon viser besøk knyttet til politisk eller religiøs utøvelse. |
|  |

|  |
| --- |
| Virksomheter med ansvar og deres rolle i behandlingsaktiviteten (behandlingsansvar, databehandlere og ev. felles behandlingsansvar) |
| Virksomhet | Rolle | Beskrivelse av oppgave/aktivitet |
|  | Behandlingsansvarlig |  |
|  | Databehandler |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Foreligger felles behandlingsansvar? Gi i en beskrivelse av eventuelle felles behandlingsansvarlige og hvilke behandlingsaktiviteter som er felles ansvar. |
|  |
| Beskriv eventuelle andre relevante aktører i tilknytning til behandlingen og grensen mellom deres og vårt ansvar (For eksempel om behandlingsaktiviteten står i en større sammenheng hvor andre offentlige aktører inngår og bør forklares. Dette kan være samarbeid mot arbeidslivskriminalitet, samarbeid med NAV eller lærebedrifter.) |
|  |

|  |
| --- |
| Hvilke personopplysninger behandles og hvem behandles det personopplysninger om? |
| Beskriv hvilke kategorier av registrerte og hvilke personopplysninger som behandles. Oppføringen skal være uttømmende.* Vurderinger/kvalitative beskrivelser er også personopplysninger
* Angi i feltet for utdypning dersom det er betydelige forskjeller på omfang eller hvilke personopplysninger som behandles om ulike individer innenfor samme kategori registrerte. (Eks «lagres kun om et lite mindretall som har behov for særskilt tilpasning»)
* Husk eventuelle personopplysninger som genereres i behandlingen uten direkte knytning til behandlingens formål, som personopplysninger i IT-logger eller andre personopplysninger som genereres som følge av sikkerhetstiltak knyttet til aktuelt system eller behandling, utilsiktet «tilleggsfangst» som f.eks. ved videoovervåkning m.m.
 |
| Kategori av registrerte | Kategori personopplysninger | Særlige kategorier av personopplysninger iht. artikkel 9 | Utdypning/beskrivelse |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Omfatter behandlingsaktiviteten opplysninger om sårbare registrerte? (f.eks. barn, psykisk syke, pasienter). Hvilke grupper gjelder dette? |
|  |
| Omfatter behandlingsaktiviteten opplysninger om straffedommer eller lovovertredelser iht. artikkel 10. Beskriv hvilke kategorier registrerte og hvilke kategorier opplysninger dette er snakk om. |
|  |

|  |
| --- |
| Hvem/hvor kommer personopplysningene fra? |
| Hvor kommer personopplysningene fra og hvordan blir opplysningene samlet inn og registrert? Hvordan lagres personopplysningene? Hvor lagres personopplysningene? I hvilken form lages data (strukturert, ikke-strukturert)? Ta også med eventuell lagring i analog form (papir). |
| Hvor kommer opplysningene fra (kilde)? | Hvordan samles personopplysningene inn fra kilden?  | Hvilke personopplysninger kommer fra denne kilden? | Hvordan lagres personopplysningene? |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| Oppdatering, endring og retting |
| Beskriv hvordan personopplysningene endres, oppdateres eller rettes. Beskriv hva som er automatisert og hva som må gjøres manuelt. Ta med eventuelle rutiner og prinsipper. Bruk gjerne vedlegg om det er praktisk. |
|  |

|  |
| --- |
| Sletting, destruksjon eller anonymisering  |
| Beskriv når eller etter hvilket mønster/frekvens personopplysninger systematisk slettes, destrueres og/eller anonymiseres?  |
|  |
| Beskriv hvordan personopplysninger slettes, destrueres og/eller anonymiseres?Beskriv rutiner og midler, slik som metode eller logikk for automatisert sletting, manuell sletting, anonymisering av digital informasjon, destruksjon av analogt eller digitalt lagrede personopplysninger.  |
|  |
| Beskriv mulighet for enkeltstående sletting, f.eks. etter begjæring fra registrert. |
|  |

|  |
| --- |
| Tilgang til personopplysningene  |
| Beskriv hvem (grupper og roller) som skal ha tilgang til personopplysninger innenfor behandlingsansvarlig organisasjon. Beskriv rutiner og midler for tilgangsstyring. Beskriv tilganger hos og føringer til eventuell databehandler. Bruk gjerne vedlegg om det er praktisk. |
|  |

|  |
| --- |
| Utlevering til tredjeparter – selvstendig behandlingsansvarlige |
| Utleveres personopplysninger til tredjeparter utenfor virksomheten som er selvstendige behandlingsansvarlige? Beskriv parter, hva som utleveres til hvem og frekvens/systematikken i utleveringen. Dersom det er aktuelt, skriv også inn parter som det sannsynligvis vil bli utlevert personopplysninger til i mer enkeltstående tilfeller, slik som utleveringsbegjæringer fra politiet eller andre myndigheter, offentlighet og innsynskrav, med videre. |
|  |

|  |
| --- |
| Overføring til tredjeland (overføring eller tilgjengeliggjøring til land utenfor EU/EØS) |
| Overføres eller på annen måte tilgjengeliggjøres personopplysninger til forhåndsgodkjente land (se ordliste)? |
|  |
| Overføres eller på annen måte tilgjengeliggjøres personopplysninger til internasjonal organisasjon? |
|  |
| Overføres eller på annen måte tilgjengeliggjøres personopplysninger til øvrige land utenfor EU/EØS? |
|  |
| *Eventuell overføring til forhåndsgodkjent land, internasjonal organisasjon eller land utenfor EU/EØS skal dokumenteres eget bilag med hvilke overføringsgrunnlag man ev. planlegger å bruke.*  |

|  |
| --- |
| Dataflyt og integreringer |
| Visuelt kart eller beskrivelse over integrasjoner og dataflyt basert på kilder, mottakere, tilgang, overføring, utveksling og lagring. |
|  |

|  |
| --- |
| Sikring av personopplysningene (personopplysningssikkerhet) |
| Beskrivelse av sikkerhetstiltak ved behandlingen (ISO 29101 6.2 Phases of the PII processing life cycle).  |
| Hvordan er personopplysningene sikret ved innsamling? |
|  |
| Hvordan er personopplysningene sikret ved overføring? |
|  |
| Hvordan er personopplysningene sikret ved bruk? |
|  |
| Hvordan er personopplysningene sikret ved lagring? |
|  |
| Hvordan avhendes/slettes personopplysningene og hvordan er de sikret i denne prosessen? |
|  |

## Lovlighet

Behandling av personopplysninger er lovlig kun dersom det foreligger et lovlig grunnlag for behandling i henhold til personvernforordningen artikkel 6 (og eventuelt 9 ved behandling av særlige kategorier personopplysninger, se neste tabell). Større prosesser kan omfatte flere behandlingsaktiviteter med ulike behandlingsgrunnlag.

|  |  |  |  |
| --- | --- | --- | --- |
| **Behandlingsgrunnlag**  | Beskriv behandlingsaktiviteten  |  | Besvarelse/utdypning |
| Samtykke(6.1.a) |  | Hvordan er krav til samtykke planlagt ivaretatt? |  |
| Nødvendig for å oppfylle en avtale(6.1.b) |  | Hvilken avtale henvises det til? |  |
| Nødvendig for å oppfylle en rettslig forpliktelse(6.1.c) |  | Oppgi supplerende rettsgrunnlag (ofte hjemmel i lov eller forskrift – oppgi konkret hjemmel). |  |
| Nødvendig for å verne den registrerte eller annen fysisk persons vitale interesser(6.1.d) |  | Hvilke vitale interesser skal ivaretas? |  |
| Nødvendig for å utfylle en oppgave i allmenhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt(6.1.e) |  | Oppgi supplerende rettsgrunnlag (ofte hjemmel i lov eller forskrift – oppgi konkret hjemmel). | . |
| Berettiget interesse(6.1.f) |  | Oppgi den berettigede interessen og interesseavveiningen.  |  |

Behandling av særlige kategorier personopplysninger er kun lovlig dersom et av de følgende unntak er oppfylt iht. personopplysningsloven artikkel 9.

|  |  |  |  |
| --- | --- | --- | --- |
| Unntak for behandling av særlige kategorier personopplysninger  | **Beskriv behandlingsaktiviteten**  |  | **Besvarelse/utdypning** |
| **Samtykke**(9.2.a) |  | Hvordan er krav til samtykke planlagt ivaretatt?  |  |
| **Nødvendig for å oppfylle forpliktelser og utøve rettigheter** på området arbeidsrett, trygderett og sosialrett(9.2.b) |  | Angi rettslig grunnlag (vis til relevante bestemmelser i f.eks. arbeidsmiljøloven) |  |
| **Nødvendig for å verne den registrerte eller annen fysisk persons vitale interesser**, dersom den registrerte ikke er i stand til å gi samtykke(9.2.c) |  | Hvilke vitale interesser skal vernes? |  |
| **Behandlingen utføres av stiftelse, sammenslutning eller ideelt organ** hvis mål er av politisk, religiøs eller fagforeningsmessig art, som ledd i organets berettigede aktiviteter og med nødvendige garantier, forutsatt at behandlingen bare gjelder organets medlemmer eller tidligere medlemmer eller personer som på grunn av organets mål har regelmessig kontakt med det, og at personopplysninger ikke kan utleveres til andre enn nevnte organ uten de registrertes samtykke(9.2.d) |  |  |  |
| **Behandlingen gjelder opplysninger som det er åpenbart at den registrerte har offentliggjort**(9.2.e) |  | Hvor/hvordan er opplysningene offentliggjort? |  |
| **Nødvendig for å fastsette, gjøre gjeldende eller forsvare rettskrav** eller når domstolene handler innenfor rammen av sin domsmyndighet(9.2.f) |  | Hvilket eller hvilke rettskrav? |  |
| **Nødvendig av hensyn til viktige allmenne interesser**, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede tekniske og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser(9.2.g) |  | Hvilke interesser?Oppgi rettsgrunnlag (ofte hjemmel i lov eller forskrift – oppgi konkret hjemmel). |   |
| **Nødvendig i forbindelse med:** **- yting av helse- og sosialtjenester** **- forebyggende medisin eller arbeidsmedisin for å vurdere en arbeidstakers arbeidskapasitet** **- medisinsk diagnostikk** **- behandling eller forvaltning av helse- eller sosialtjenester og –systemer**på grunnlag av unionsretten eller medlemsstatenes nasjonale rett eller i henhold til en avtale med helsepersonell og med forbehold om vilkårene og garantiene nevnt i nr. 3(9.2.h) |  | Oppgi rettsgrunnlag (ofte hjemmel i lov eller forskrift – oppgi konkret hjemmel). |  |
| **Nødvendig av allmenne folkehelsehensyn** på grunnlag av unionsretten eller medlemsstatenes nasjonale rett der det fastsettes egnede og særlige tiltak for å verne den registrertes rettigheter og friheter, særlig taushetsplikt(9.2.i) |  | Hvilke allmenne folkehelsehensyn?Oppgi rettsgrunnlag (ofte hjemmel i lov eller forskrift – oppgi konkret hjemmel). |  |
| **Nødvendig for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1**, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser(9.2.j) |  | Hvilke formål?Oppgi rettsgrunnlag (ofte hjemmel i lov eller forskrift – oppgi konkret hjemmel). |  |

|  |
| --- |
| Informasjon, åpenhet og håndtering av rettigheter |
| Beskriv hvordan krav om åpenhet om behandlingen og informasjon til registrerte blir ivaretatt (f.eks. personvernerklæring på nettsidene, annen informasjon, opplæring m.m.) |
|  |
| Beskriv hvordan den registrerte blir informert om sine personvernrettigheter i forbindelse med behandlingen? |
|  |
| Beskriv hvordan krav om rettigheter kan inngis, bistand til registrerte, samt organisatoriske og tekniske elementer i inngivelse og behandling av rettigheter. |
|  |

|  |
| --- |
| Dokumentasjon - vedleggKryss av etter hva som er aktuelt. Legg til etter ønske. |
|  | Vurdering av rettslig grunnlag for behandlingen og eventuelt sekundært rettsgrunnlag |
|  | Interesseavveining |
|  | Samtykkeerklæring |
|  | Personvernerklæring |
|  | Vurdering av tredjelandsoverføring |
|  | Annet |

#

# VURDERING AV RISIKOER OG TILTAK

Vurderingen tar for seg forordningens prinsipper etter artikkel 5, de registrertes rettigheter etter artikkel 12 til 22 samt de registrertes rettigheter og friheter som følger av blant annet den europeiske menneskerettighetskonvensjon, FNs konvensjoner om henholdsvis sivile og politiske rettigheter og økonomiske, sosiale og kulturelle rettigheter.

Formålet er å avklare hvorvidt disse kravene i personvernforordningen etterleves, om det foreligger risikoer knyttet til de angitte områdene samt identifisering av tiltak for å redusere vesentlige risikoer og sikre at kravene etterleves.

Spørsmålene vil være til hjelp med vurderingen og kan benyttes i den grad de ansees som relevante. De vil kunne bidra til å identifisere utfordringer eller risikoer. Spørsmålene er ikke utfyllende, andre relevante forhold eller problemstillinger kan angis og besvares etter behov.

Man kan benytte eget risikovurderingsverktøy og overføre vesentlige risikoer derifra.

## PERSONVERNPRINSIPPENE

Personopplysningsloven med personvernforordningen inneholder både rettigheter og plikter. Felles for alle reglene er at de bygger på de grunnleggende prinsippene i personvernforordningen artikkel 5.

### Lovlighet

Behandling av personopplysninger er bare lovlig dersom behandlingen har behandlingsgrunnlag i artikkel 6 nr. 1. Behandling av særlige kategorier av personopplysninger må i tillegg oppfylle ett av unntakene i artikkel 9 nr. 2.

Lovlighetsprinsippet handler om mer enn behandlingsgrunnlag – behandlingen må også oppfylle andre krav i regelverket. Malen her konsentrerer seg primært om behandlingsgrunnlag og vilkår for å behandle særlige kategorier av personopplysninger. Andre temaer om lovlighet kan legges inn dersom det er ønskelig.

|  |
| --- |
| **SPØRSMÅL** |
| Dekker behandlingsgrunnlaget det eller de definerte formålet med behandlingen? |
|  |
| Dekker behandlingsgrunnlaget alle kategorier personopplysninger som inngår i behandlingen, også særlige kategorier der det er aktuelt? |
|  |
| Dekker behandlingsgrunnlaget alle operasjoner av personopplysningene (også ev. utlevering av personopplysningene)? |
|  |
| Er vilkårene for behandlingsgrunnlaget oppfylt? Er f.eks. kravene til et gyldig samtykke oppfylt eller interesseavveiing utført der dette er påkrevd. |
|  |
| Er du kjent med at behandlingsaktiviteten omfattes av annen lov eller regelverk som bør vurderes? Dette kan være sikkerhetslov, regnskapslov eller andre lover som stiller krav til behandlingsaktiviteten. |
|  |
| Er det andre forhold eller utfordringer som er vesentlig å anmerke? |
|  |

|  |
| --- |
|  |
| **RISIKO** |
| Risiko ID | Risikoformulering | Risiko ved vurderingstidspunkt | Estimert risiko etter nødvendige og anbefalte tiltak |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |
| **TILTAK**Beskrivelse av tiltak som er nødvendig eller anbefalt for å kunne anse kravet som ivaretatt. |
| Tiltak ID | Tiltak | Nødvendig eller anbefalt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |

|  |
| --- |
|  |
| **VURDERING – LOVLIGHET** |
| Ansees prinsippet lovlighet som ivaretatt i behandlingen?Kravet kan ansees som ivaretatt der det ikke er identifiserte risikoer utenfor akseptabelt risikonivå eller er avdekket øvrige forhold som tilsier at lovkravet ikke kan etterleves. |
| Kryss av for aktuelt svar | Nærmere forklaring |
| [ ]  | Ja |  |
| [ ]  | Ja, under forutsetning av gjennomføring av oppgitte tiltak |  |
| [ ]  | Usikkert om kravet kan etterleves |  |
| [ ]  | Nei |  |

###

### Rettferdighet

Behandlingen av personopplysninger må gjøres i respekt for de registrertes interesser og rimelige forventninger. Behandlingen skal være forståelig for de registrerte og ikke foregå på skjulte eller manipulerende måter. Rettferdighet ivaretas også i andre prinsipper slik som f.eks. åpenhet og lovlighet.

|  |
| --- |
| **SPØRSMÅL** |
| Er det vurdert hvordan behandlingsaktiviteten kan påvirke de berørte personene og kan eventuelle negative konsekvenser rettferdiggjøres? |
|  |
| Behandles personopplysninger med respekt for de registrertes interesser og slik de med rimelighet kan forvente? |
|  |
| Manipuleres eller på andre måter villedes de registrerte eller andre berørte slik personopplysningene samles inn og behandles for øvrig? |
|  |
| Har den registrerte størst mulig grad av selvbestemmelse i forhold til bruken av deres personlige data? |
|  |
| Brukes press, tvang eller store positive eller negative konsekvenser som virkemidler overfor den registrerte? Kan dette i så fall forsvares? |
|  |
| Er det andre forhold eller utfordringer som er vesentlig å anmerke? |
|  |
|  |
| **RISIKO** |
| Risiko ID | Risikoformulering | Risiko ved vurderingstidspunkt | Estimert risiko etter nødvendige og anbefalte tiltak |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |
| **TILTAK**Beskrivelse av tiltak som er nødvendig eller anbefalt for å kunne anse kravet som ivaretatt. |
| Tiltak ID | Tiltak | Nødvendig eller anbefalt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |
| **VURDERING – RETTFERDIGHET** |
| Ansees prinsippet rettferdighet som ivaretatt i behandlingsaktiviteten?Kravet kan ansees som ivaretatt der det ikke er identifiserte risikoer utenfor akseptabelt risikonivå eller er avdekket øvrige forhold som tilsier at lovkravet ikke kan etterleves. |
| Kryss av for aktuelt svar | Nærmere forklaring |
| [ ]  | Ja |  |
| [ ]  | Ja, under forutsetning av gjennomføring av oppgitte tiltak |  |
| [ ]  | Usikkert om kravet kan etterleves |  |
| [ ]  | Nei |  |

### Åpenhet

Behandling av personopplysninger skal være tilgjengelig, oversiktlig og forutsigbar for den registrerte. Åpenhet bidrar til å skape tillit og det setter den registrerte i stand til å bruke sine rettigheter og ivareta sine interesser.

Vurdering av åpenhet skal ivareta alle kategorier registrerte og de kategorier personopplysninger som er knyttet til de registrerte.

Den registrertes rett til informasjon iht. artikkel 12, 13 og 14 beskrives senere under punktet De registrertes rettigheter – rett til informasjon.

|  |
| --- |
| **SPØRSMÅL** |
| Vil den registrerte kjenne til og forstå hvordan sine personopplysninger behandles? |
|  |
| Behandles opplysninger utover det som er synlig/åpent for registrerte – f.eks. opplysninger fra andre parter eller systemgenererte data? |
|  |
| Er registrerte tilstrekkelig kjent med om behandlingens formål, herunder om de benyttes til andre eller nye formål? |
|  |
| Behandles personopplysninger på en måte som er uventet eler vanskelig å forstå for den registrerte, og som heller ikke formidlet og forklart? Herunder også gjennom profilering, automatiserte beslutninger eller eventuell viderebehandling som ikke er åpenbar for den registrerte. |
|  |
| Er det andre forhold eller utfordringer som er vesentlig å anmerke? |
|  |

|  |
| --- |
|  |
| **RISIKO** |
| Risiko ID | Risikoformulering | Risiko ved vurderingstidspunkt | Estimert risiko etter nødvendige og anbefalte tiltak |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |
| **TILTAK**Beskrivelse av tiltak som er nødvendig eller anbefalt for å kunne anse kravet som ivaretatt. |
| Tiltak ID | Tiltak | Nødvendig eller anbefalt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |

|  |
| --- |
| **VURDERING – ÅPENHET** |
| Ansees prinsippet åpenhet som ivaretatt i behandlingsaktiviteten?Kravet kan ansees som ivaretatt der det ikke er identifiserte risikoer utenfor akseptabelt risikonivå eller er avdekket øvrige forhold som tilsier at lovkravet ikke kan etterleves. |
| Kryss av for aktuelt svar | Nærmere forklaring |
| [ ]  | Ja |  |
| [ ]  | Ja, under forutsetning av gjennomføring av oppgitte tiltak |  |
| [ ]  | Usikkert om kravet kan etterleves |  |
| [ ]  | Nei |  |

###

### Formålsbegrensning

Personopplysninger kan kun behandles for spesifikke, uttrykkelig angitte og berettigede formål.

Vurderingen av personvernkonsekvenser kan omfatte flere sammenfallende behandlinger og kan derfor også omfatte flere formål og underformål.

|  |
| --- |
| **SPØRSMÅL** |
| Behandles personopplysningene for behandles for spesifikke, uttrykkelige angitte og berettigede formål? |
|  |
| Er formålet definert slik at det samsvarer med forventingene den registrerte har til behandlingen? |
|  |
| Er formålet formulert på en måte som gjør det enkelt å forstå hva som er innenfor og utenfor formålet? |
|  |
| Viderebehandles personopplysningene på en måte som ikke er forenelig med de oppgitte formålene? |
|  |
| Kan behandlingsansvarlig ivareta sine behov med et mindre inngripende mer begrenset/snevert formål? |
|  |
| Er det andre forhold eller utfordringer som er vesentlig å anmerke? |
|  |

|  |
| --- |
|  |
| **RISIKO** |
| Risiko ID | Risikoformulering | Risiko ved vurderingstidspunkt | Estimert risiko etter nødvendige og anbefalte tiltak |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |
| **TILTAK**Beskrivelse av tiltak som er nødvendig eller anbefalt for å kunne anse kravet som ivaretatt. |
| Tiltak ID | Tiltak | Nødvendig eller anbefalt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |

|  |
| --- |
| **VURDERING – FORMÅLSBEGRENSNING** |
| Ansees prinsippet formålsbegrensning som ivaretatt i behandlingsaktiviteten?Kravet kan ansees som ivaretatt der det ikke er identifiserte risikoer utenfor akseptabelt risikonivå eller er avdekket øvrige forhold som tilsier at lovkravet ikke kan etterleves. |
| Kryss av for aktuelt svar | Nærmere forklaring |
| [ ]  | Ja |  |
| [ ]  | Ja, under forutsetning av gjennomføring av oppgitte tiltak |  |
| [ ]  | Usikkert om kravet kan etterleves | . |
| [ ]  | Nei |  |

###

### Dataminimering

Mengden innsamlede personopplysninger skal begrenses til det som er nødvendig for å oppnå formålet med behandlingsaktiviteten. Dette setter krav til å unngå overskuddsinformasjon – personopplysningene må være adekvate og relevante.

Begrensing av mengden innsamlede personopplysninger krever oversikt over opplysningene som samles inn og formålet for behandlingsaktiviteten.

|  |
| --- |
| **SPØRSMÅL** |
| Er personopplysningene som behandles adekvate og relevante for formålet |
|  |
| Er personopplysningene som behandles begrenset til det som er nødvendig for formålet? |
|  |
| Kan formålet oppnås ved innhenting av færre personopplysninger? |
|  |
| Kan formålet oppnås uten bruk av personopplysninger, eller med pseudonymiserte, anonymiserte eller aggregerte opplysninger? |
|  |
| Er tilgangen til begrenset til de som trenger den for å utføre sine oppgaver? |
|  |
| Er det andre forhold eller utfordringer som er vesentlig å anmerke? |
|  |
|  |
| **RISIKO** |
| Risiko ID | Risikoformulering | Risiko ved vurderingstidspunkt | Estimert risiko etter nødvendige og anbefalte tiltak |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |
| **TILTAK**Beskrivelse av tiltak som er nødvendig eller anbefalt for å kunne anse kravet som ivaretatt. |
| Tiltak ID | Tiltak | Nødvendig eller anbefalt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |
| **VURDERING – DATAMINIMERING** |
| Ansees prinsippet dataminimering som ivaretatt i behandlingsaktiviteten?Kravet kan ansees som ivaretatt der det ikke er identifiserte risikoer utenfor akseptabelt risikonivå eller er avdekket øvrige forhold som tilsier at lovkravet ikke kan etterleves. |
| Kryss av for aktuelt svar | Nærmere forklaring |
| [ ]  | Ja |  |
| [ ]  | Ja, under forutsetning av gjennomføring av oppgitte tiltak |  |
| [ ]  | Usikkert om kravet kan etterleves |   |
| [ ]  | Nei |  |

### Riktighet

Personopplysningene som behandles skal være korrekte og oppdaterte slik at de gir riktig grunnlag for vurderinger, beslutninger og handlinger. Det er derfor viktig å sørge for å slette eller rette uriktige opplysninger gjennom hele behandlingens forløp.

|  |
| --- |
| **SPØRSMÅL** |
| Er datakildene pålitelige slik at dataunderlaget har høy kvalitet? |
|  |
| Foreligger tilstrekkelige tekniske og organisatoriske tiltak for å holde personopplysningene korrekte og oppdaterte? |
|  |
| Har den registrerte anledning til å oppdatere opplysninger eller korrigere uriktige opplysninger? |
|  |
| Foreligger tilstrekkelige logger slik at uønskede endringer eller slettinger kan spores? |
|  |
| Er tilgangsstyring og rettigheter slik at muligheten for ukvalifiserte eller uønskede rettinger eller slettinger begrenses? |
|  |
| Er det andre forhold eller utfordringer som er vesentlig å anmerke? |
|  |
|  |
| **RISIKO** |
| Risiko ID | Risikoformulering | Risiko ved vurderingstidspunkt | Estimert risiko etter nødvendige og anbefalte tiltak |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |
| **TILTAK**Beskrivelse av tiltak som er nødvendig eller anbefalt for å kunne anse kravet som ivaretatt. |
| Tiltak ID | Tiltak | Nødvendig eller anbefalt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |
| **VURDERING – RIKTIGHET** |
| Ansees riktighet som ivaretatt i behandlingsaktiviteten?Kravet kan ansees som ivaretatt der det ikke er identifiserte risikoer utenfor akseptabelt risikonivå eller er avdekket øvrige forhold som tilsier at lovkravet ikke kan etterleves. |
| Kryss av for aktuelt svar | Nærmere forklaring |
| [ ]  | Ja |  |
| [ ]  | Ja, under forutsetning av gjennomføring av oppgitte tiltak |  |
| [ ]  | Usikkert om kravet kan etterleves |  |
| [ ]  | Nei |  |

### Lagringsbegrensning

Personopplysninger skal lagres slik at de slettes eller anonymiseres når de ikke lengre er nødvendige for formålet de ble innhentet for. Det skal gjennom hele behandlingen foreligge behandlingsgrunnlag iht. artikkel 6 (og evt. også artikkel 9). Når behandlingsgrunnlaget ikke lenger foreligger skal behandlingen avsluttes dersom nytt behandlingsgrunnlag ikke er identifisert.

Tidsrommet eller kriteriene for lagring eller anonymisering skal være dokumentert og etterlevet.

Lagringsbegrensning omfatter alle kategorier personopplysninger som behandles og inkluderer også sikkerhetskopier, e-post, mellomlagring, skylagring m.m.

|  |
| --- |
| **SPØRSMÅL** |
| Behandles personopplysninger slik at det er mulig å identifisere den registrerte i en lengre periode enn det som er nødvendig for formålene de behandles for eller behandlingsgrunnlaget gir adgang til? |
|  |
| Er tidsrommet opplysningene vil bli lagret eller kriteriene som brukes for å fastsette dette tidsrommet, fastsatt og dokumentert i tilstrekkelig grad? |
|  |
| Lagres personopplysningene lenger enn de definerte formålene knyttet til arkiv eller forskningsformål (jf. art. 89)? |
|  |
| Har tjenesten eller løsningen funksjonalitet for å ivareta kriteriene som er satt for lagringsbegrensning – kan opplysningene faktisk slettes? |
|  |
| Er lagringsbegrensing tilstrekkelig ivaretatt i backup- løsninger, logger, midlertidige lagringssteder eller tilsvarende? |
|  |
| Er det andre forhold eller utfordringer som er vesentlig å anmerke? |
|  |
|  |
| **RISIKO** |
| Risiko ID | Risikoformulering | Risiko ved vurderingstidspunkt | Estimert risiko etter nødvendige og anbefalte tiltak |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |
| **TILTAK**Beskrivelse av tiltak som er nødvendig eller anbefalt for å kunne anse kravet som ivaretatt. |
| Tiltak ID | Tiltak | Nødvendig eller anbefalt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |
| **VURDERING – LAGRINGSBEGRENSING** |
| Ansees lagringsbegrensing som ivaretatt i behandlingsaktiviteten?Kravet kan ansees som ivaretatt der det ikke er identifiserte risikoer utenfor akseptabelt risikonivå eller er avdekket øvrige forhold som tilsier at lovkravet ikke kan etterleves. |
| Kryss av for aktuelt svar | Nærmere forklaring |
| [ ]  | Ja |  |
| [ ]  | Ja, under forutsetning av gjennomføring av oppgitte tiltak |  |
| [ ]  | Usikkert om kravet kan etterleves |  |
| [ ]  | Nei |  |

### Integritet og konfidensialitet

Integritet og konfidensialitet skal sikres gjennom egnede tekniske og organisatoriske tiltak slik at sikkerheten ivaretas i henhold til den risiko behandlingen utgjør.

Personopplysningssikkerheten ivaretas ved at konfidensialitet, tilgjengelighet og integritet ivaretas og robusthet sikres ved behandlingen av personopplysninger i henhold til krav i artikkel 5, 24 og 32.

Risikoer knyttet til konfidensialitet, integritet og tilgjengelighet vil normalt vurderes i en ordinær risikovurdering slik at spørsmålene kan besvares og vesentlige risikoer med tiltak registreres her.

|  |
| --- |
| **SPØRSMÅL** |
| Er personopplysningene tilstrekkelig sikret mot uautorisert eller ulovlig behandling? |
|  |
| Er personopplysningene tilstrekkelig sikret mot utilsiktet tap, ødeleggelse eller skade? |
|  |
| Er tekniske tiltak definert for å ivareta et tilstrekkelig sikkerhetsnivå ved behandlingsaktiviteten? |
|  |
| Er organisatoriske tiltak definert for å ivareta et tilstrekkelig sikkerhetsnivå ved behandlingsaktiviteten? |
|  |
| Er det gjennomført risikovurdering hvor personopplysningssikkerhet inngår? |
|  |
| Viser gjennomført risikovurdering for personopplysningssikkerheten risikoer utover akseptabelt sikkerhetsnivå? |
|  |
| Er det andre forhold eller utfordringer som er vesentlig å anmerke? |
|  |
|  |
| **RISIKO** |
| Risiko ID | Risikoformulering | Risiko ved vurderingstidspunkt | Estimert risiko etter nødvendige og anbefalte tiltak |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |
| **TILTAK**Beskrivelse av tiltak som er nødvendig eller anbefalt for å kunne anse kravet som ivaretatt. |
| Tiltak ID | Tiltak | Nødvendig eller anbefalt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |
| **VURDERING – KONFIDENSIALITET OG INTEGRITET** |
| Ansees konfidensialitet og integritet som ivaretatt i behandlingsaktiviteten?Kravet kan ansees som ivaretatt der det ikke er identifiserte risikoer utenfor akseptabelt risikonivå eller er avdekket øvrige forhold som tilsier at lovkravet ikke kan etterleves. |
| Kryss av for aktuelt svar | Nærmere forklaring |
| [ ]  | Ja |  |
| [ ]  | Ja, under forutsetning av gjennomføring av oppgitte tiltak |  |
| [ ]  | Usikkert om kravet kan etterleves |  |
| [ ]  | Nei |  |

## REGISTRERTES RETTIGHETER

Målet med denne delen av vurderingen er å ta stilling til om de registrerte vil få de rettigheter de har krav på, hvilken risiko vi står overfor og hva vi eventuelt må gjøre for at rettigheter skal bli ivaretatt på en god måte.

### Oversikt over relevante rettigheter ifm. behandlingsaktiviteten

Huk av og forklar dersom noen av rettighetene under ikke er relevante for den aktuelle behandlingsaktiviteten. Dette er rettigheter som initieres av den registrerte. Rett til informasjon er behandlingsansvarliges ansvar.

|  |  |  |
| --- | --- | --- |
| **Kryss dersom ikke relevant** | **Rettighet** | **Forklaring på hvorfor rettigheten ikke aktuell** |
|  | Rett til innsyn |  |
|  | Rett til retting |  |
|  | Rett til sletting |  |
|  | Rett til begrensning |  |
|  | Rett til å protestere Gjelder kun ved myndighetsutøvelse (6.1.e) og berettiget interesse (6.1.f) |  |
|  | Rettigheter ved automatiserte avgjørelser |  |
|  | Rett til dataportabilitetGjelder kun ved samtykke (6.1.a) og avtale (6.1.b) |  |

### Generell behandling av rettighetsforespørsler

|  |
| --- |
| **SPØRSMÅL** |
| Har virksomheten kompetanse til å identifisere og behandle krav fra registrerte om rettigheter som innsyn, retting, sletting, protest eller dataportabilitet? |
|  |
| Vil en registrert får riktig veiledning om rettigheter og hvordan disse kan inngis? |
|  |
| Har virksomheten rutiner og praksis som ivaretar riktig saksbehandling innenfor tidsfristene ved en rettighetsforespørsel fra registrerte? |
|  |
| Har virksomheten hensiktsmessige løsninger for å verifisere at innsender av rettighetskrav er den vedkommende utgir seg for? |
|  |
|  |
| **RISIKO** |
| Risiko ID | Risikoformulering | Risiko ved vurderingstidspunkt | Estimert risiko etter nødvendige og anbefalte tiltak |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |
| **TILTAK**Beskrivelse av tiltak som er nødvendig eller anbefalt for å kunne anse kravet som ivaretatt. |
| Tiltak ID | Tiltak | Nødvendig eller anbefalt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |
| **VURDERING – GENERELLE RETTIGHTER** |
| Ansees virksomheten som i stand til å håndtere rettighetsforespørsler?Kravet kan ansees som ivaretatt der det ikke er identifiserte risikoer utenfor akseptabelt risikonivå eller er avdekket øvrige forhold som tilsier at lovkravet ikke kan etterleves. |
| Kryss av for aktuelt svar | Nærmere forklaring |
| [ ]  | Ja |  |
| [ ]  | Ja, under forutsetning av gjennomføring av oppgitte tiltak |  |
| [ ]  | Usikkert om kravet kan etterleves |  |
| [ ]  | Nei |  |

### Rett til informasjon

Den behandlingsansvarlige skal gi den registrerte informasjon om behandlingsaktiviteten i henhold til artikkel 13 og 14.

|  |
| --- |
| **SPØRSMÅL** |
|  |
| Foreligger informasjon til registrerte om behandlingsaktiviteten? |
|  |
| Er informasjonen lett tilgjengelig på riktig tidspunkt og kan du finne den igjen senere? |
|  |
| Er den utformet på en kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk? |
|  |
| Dersom registrerte omfatter barn eller andre sensitive grupper, er informasjonen tilpasset disse? |
|  |
| Er informasjonen i samsvar med de øvrige kravene til innhold slik angitt i artikkel 13 og 14? |
|  |
| Er det andre forhold eller utfordringer som er vesentlig å anmerke? |
|  |
|  |
| **RISIKO** |
| Risiko ID | Risikoformulering | Risiko ved vurderingstidspunkt | Estimert risiko etter nødvendige og anbefalte tiltak |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |
| **TILTAK**Beskrivelse av tiltak som er nødvendig eller anbefalt for å kunne anse kravet som ivaretatt. |
| Tiltak ID | Tiltak | Nødvendig eller anbefalt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |
| **VURDERING – RETT TIL INFORMASJON** |
| Ansees rettigheten som ivaretatt i behandlingsaktiviteten?Kravet kan ansees som ivaretatt der det ikke er identifiserte risikoer utenfor akseptabelt risikonivå eller er avdekket øvrige forhold som tilsier lovkravet ikke kan etterleves. |
| Kryss av for aktuelt svar | Nærmere forklaring |
| [ ]  | Ja |  |
| [ ]  | Ja, under forutsetning av gjennomføring av oppgitte tiltak |  |
| [ ]  | Usikkert om kravet kan etterleves |  |
| [ ]  | Nei |  |

### Rett til innsyn

Den registrerte har rett til innsyn i behandlingen av personopplysninger som foretas om seg selv. Dette omfatter blant annet rett til å få informasjon om formålet ved behandlingen, hvilke opplysninger som behandles og når de slettes. Rett til innsyn initieres av registrerte.

|  |
| --- |
| **SPØRSMÅL** |
| Har den registrerte fått informasjon om sin rett til innsyn? |
|  |
| Foreligger rutiner og ansvar for håndtering av rettigheten? |
|  |
| Kan de registrerte selv finne informasjon om behandlingen og hva som er lagret om vedkommende, for eksempel ved hjelp av «min side» eller liknende i et datasystem? |
|  |
| Vil manglede oversikt, uklare interne ansvarsforhold, tekniske begrensninger eller andre forhold gjøre at en registrert kun får tilsendt kopi av noen av de personopplysningene eller kategorier personopplysninger som faktisk behandles om vedkommende. |
|  |
| Er det andre forhold eller utfordringer som er vesentlig å anmerke? |
|  |
|  |
| **RISIKO** |
| Risiko ID | Risikoformulering | Risiko ved vurderingstidspunkt | Estimert risiko etter nødvendige og anbefalte tiltak |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |
| **TILTAK**Beskrivelse av tiltak som er nødvendig eller anbefalt for å kunne anse kravet som ivaretatt. |
| Tiltak ID | Tiltak | Nødvendig eller anbefalt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |
| **VURDERING – RETT TIL INNSYN** |
| Ansees rettigheten som ivaretatt i behandlingsaktiviteten?Kravet kan ansees som ivaretatt der det ikke er identifiserte risikoer utenfor akseptabelt risikonivå eller er avdekket øvrige forhold som tilsier at lovkravet ikke kan etterleves. |
| Kryss av for aktuelt svar | Nærmere forklaring |
| [ ]  | Ja |  |
| [ ]  | Ja, under forutsetning av gjennomføring av oppgitte tiltak |  |
| [ ]  | Usikkert om kravet kan etterleves |  |
| [ ]  | Nei |  |

### Rett til retting og sletting

Den registrerte har rett til å få slettet eller rettet opplysninger om seg selv blant annet dersom de ikke lenger er nødvendige, er feilaktige eller der hvor lovlig grunnlag for behandling ikke foreligger. Retting til retting og sletting omhandler her rettigheten som initieres av registrerte. Sletting etter behandlingsansvarliges initiativ vurderes under prinsippet om lagringsbegrensning.

|  |
| --- |
| **SPØRSMÅL** |
| Har den registrerte fått informasjon om sine rett til retting og sletting? |
|  |
| Foreligger rutiner og ansvar for håndtering av rettigheten? |
|  |
| Kan den registrerte selv slette eller endre sine personopplysninger, for eksempel via muligheter i systemet? |
|  |
| Er det teknisk mulig å rette eller slette enkelte personopplysninger dersom den registrerte stiller rettmessig krav om dette? |
|  |
| Er det andre forhold eller utfordringer som er vesentlig å anmerke? |
|  |
|  |
| **RISIKO** |
| Risiko ID | Risikoformulering | Risiko ved vurderingstidspunkt | Estimert risiko etter nødvendige og anbefalte tiltak |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |
| **TILTAK**Beskrivelse av tiltak som er nødvendig eller anbefalt for å kunne anse kravet som ivaretatt. |
| Tiltak ID | Tiltak | Nødvendig eller anbefalt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |
| **VURDERING – RETT TIL RETTING OG SLETTING** |
| Ansees rettigheten som ivaretatt i behandlingsaktiviteten?Kravet kan ansees som ivaretatt der det ikke er identifiserte risikoer utenfor akseptabelt risikonivå eller er avdekket øvrige forhold som tilsier at lovkravet ikke kan etterleves. |
| Kryss av for aktuelt svar | Nærmere forklaring |
| [ ]  | Ja |  |
| [ ]  | Ja, under forutsetning av gjennomføring av oppgitte tiltak |  |
| [ ]  | Usikkert om kravet kan etterleves |  |
| [ ]  | Nei |  |

### Rett til begrensning

I noen situasjoner har den registrerte rett til at behandling av egne personopplysninger begrenses. Dette betyr at opplysningene for en periode bare lagres. Eventuell behandling utover lagring krever den registrertes samtykke eller at et annet lovbestemt unntak er oppfylt.

|  |
| --- |
| **SPØRSMÅL** |
| Har den registrerte fått informasjon om sin rett å begrense behandlingen? |
|  |
| Har virksomheten nødvendig kompetanse/forutsetninger til å saksbehandle krav om begrensning? |
|  |
| Kan retten til begrensing håndteres, er f.eks. løsningen designet for å håndtere et krav om begrensing? |
|  |
| Er det andre forhold eller utfordringer som er vesentlig å anmerke? |
|  |
|  |
| **RISIKO** |
| Risiko ID | Risikoformulering | Risiko ved vurderingstidspunkt | Estimert risiko etter nødvendige og anbefalte tiltak |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |
| **TILTAK**Beskrivelse av tiltak som er nødvendig eller anbefalt for å kunne anse kravet som ivaretatt. |
| Tiltak ID | Tiltak | Nødvendig eller anbefalt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |
| **VURDERING –RETT TIL BEGRENSING** |
| Ansees rettigheten som ivaretatt i behandlingsaktiviteten?Kravet kan ansees som ivaretatt der det ikke er identifiserte risikoer utenfor akseptabelt risikonivå eller er avdekket øvrige forhold som tilsier at lovkravet ikke kan etterleves. |
| Kryss av for aktuelt svar | Nærmere forklaring |
| [ ]  | Ja |  |
| [ ]  | Ja, under forutsetning av gjennomføring av oppgitte tiltak |  |
| [ ]  | Usikkert om kravet kan etterleves |  |
| [ ]  | Nei |  |

### Rett til å protestere

Registrerte har rett til å protestere på behandlingsaktivitet som basert på allmenhetens interesse eller utøvelse av offentlig myndighet (6.1.e) samt berettiget interesse (6.1.f).

Den behandlingsansvarlige skal ikke lenger behandle personopplysningene, med mindre virksomheten kan påvise at det foreligger tvingende berettigede grunner for behandlingen som går foran den registrertes interesser, rettigheter og friheter, eller for å fastsette, gjøre gjeldende eller forsvare rettskrav.

Den registrerte kan ha rett til å få sin behandling begrenset iht. artikkel 18.

|  |
| --- |
| **SPØRSMÅL** |
| Har den registrerte fått informasjon om sin rett å protestere mot behandlingen? |
|  |
| Har virksomheten nødvendig kompetanse/forutsetninger til å saksbehandle krav om protest? |
|  |
| Kan retten til protest håndteres, er f.eks. løsningen designet for å håndtere en protest mot behandling? |
|  |
| Er det andre forhold eller utfordringer som er vesentlig å anmerke? |
|  |
|  |
| **RISIKO** |
| Risiko ID | Risikoformulering | Risiko ved vurderingstidspunkt | Estimert risiko etter nødvendige og anbefalte tiltak |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |
| **TILTAK**Beskrivelse av tiltak som er nødvendig eller anbefalt for å kunne anse kravet som ivaretatt. |
| Tiltak ID | Tiltak | Nødvendig eller anbefalt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |
| **VURDERING – RETT TIL Å PROTESTERE**  |
| Ansees rettigheten som ivaretatt i behandlingen?Kravet kan ansees som ivaretatt der det ikke er identifiserte risikoer utenfor akseptabelt risikonivå eller er avdekket øvrige forhold som tilsier at lovkravet ikke kan etterleves. |
| Kryss av for aktuelt svar | Nærmere forklaring |
| [ ]  | Ja |  |
| [ ]  | Ja, under forutsetning av gjennomføring av oppgitte tiltak |  |
| [ ]  | Usikkert om kravet kan etterleves |  |
| [ ]  | Nei |  |

## GRUNNLEGGENDE RETTIGHETER OG FRIHETER

De registrertes rettigheter og friheter slik det er angitt i artikkel 1 følger av blant annet den europeiske menneskerettighetskonvensjon (EMK), FNs konvensjoner om henholdsvis sivile og politiske rettigheter (SP), og økonomiske, sosiale og kulturelle rettigheter (ØSK).

Det kan være forhold utover det som er avdekket under vurdering av personvernprinsipper og den registrertes rettigheter som påvirker menneskets grunnleggende friheter og rettigheter.

Her er forhold knyttet til på friheter og rettigheter som kan vurderes:

* Rett til privatliv
* Kontroll over egne personopplysninger
* Rett til ytringsfrihet
* Forskjellsbehandling eller diskriminering
* Økonomisk tap eller ulempe
* Tap av liv og helse
* Tap av omdømme eller andre sosiale ulemper
* Frihet til utøvelse av religion eller livssyn
* Frihet til politisk oppfatning og organisering

|  |
| --- |
| **SPØRSMÅL** |
| Kan behandlingen få negative virkning for ytringsfrihet, for eksempel å legge en demper på viljen til å ytre seg (nedkjølingseffekt)? |
|  |
| Kan behandlingen få negativ virkning for fri og naturlig livsutfoldelse? For eksempel ved at sporing, profilering eller følelse av overvåking reduserer viljen til å søke informasjon, ha kontakt med enkelte personer, oppsøke steder/tjenester eller ferdes fritt?  |
|  |
| Kan behandlingen redusere enkeltmenneskers mulighet for å ha kontroll over egne personopplysninger? |
|  |
| Kan behandlingen føre til urettmessig forskjellsbehandling eller diskriminering? |
|  |
| Kan behandlingen føre til økonomisk tap eller ulempe, eller redusere muligheten for å kunne leve av eget arbeid? |
|  |
| Kan behandlingen føre til tap av liv og helse? |
|  |
| Kan behandlingen krenke retten til privatliv og familieliv? |
|  |
| Kan behandlingen føre til tap av omdømme eller andre sosiale ulemper? |
|  |
| Kan behandlingen gripe inn i, eller legge bånd på fri utøvelse av religion eller livssyn? |
|  |
| Kan behandlingen redusere muligheten for, eller viljen til å engasjere seg politisk eller til å organisere seg?  |
|  |
| Er det andre forhold som er vesentlig å anmerke? |
|  |

|  |
| --- |
|  |
| **RISIKO** |
| Risiko ID | Risikoformulering | Risiko ved vurderingstidspunkt | Estimert risiko etter nødvendige og anbefalte tiltak |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |  |  Velg et element. | Velg et element. |
|  |
| **TILTAK**Beskrivelse av tiltak som er nødvendig eller anbefalt for å kunne anse den registrertes rettigheter og friheter som ivaretatt. |
| Tiltak ID | Tiltak | Nødvendig eller anbefalt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |

|  |
| --- |
| **VURDERING – RETTIGHTER OG FRIHETER** |
| Ansees registrertes rettigheter og friheter som ivaretatt i behandlingen?Kravet kan ansees som ivaretatt der det ikke er identifiserte risikoer utenfor akseptabelt risikonivå eller er avdekket øvrige forhold som tilsier at menneskers grunnleggende rettigheter og friheter ikke kan ivaretas. |
| Kryss av for aktuelt svar | Nærmere forklaring |
| [ ]  | Ja |  |
| [ ]  | Ja, under forutsetning av gjennomføring av oppgitte tiltak |  |
| [ ]  | Usikkert om kravet kan etterleves |  |
| [ ]  | Nei |  |

# VURDERING AV NØDVENDIGHET OG RIMELIGHET

I personvernkonsekvensvurdering skal det tas stilling til om behandlingsaktiviteten er nødvendig og om den står i et rimelig forhold til målet med behandlingen. Begreper som nødvendighet, proporsjonalitet (forholdsmessighet) og rimelighet står sentralt.

Å begrense seg til det nødvendige og å minimere ulemper, står sentralt i godt personvern. Dette betyr at det er viktig å ta konkret stilling til om minst mulig inngripende, men likevel fungerende løsning bli valgt.

Om behandlingen er nødvendig er knyttet til hvilken verdi eller nytte den har for den registrerte, den behandlingsansvarlige eller for samfunnet. Dette er tett knyttet til formålet for behandlingen som er beskrevet i kapittelet BESKRIVELSE AV BEHANDLINGEN.

Ved vurderingen av behandlingsaktivitetens proporsjonalitet og rimelighet veies nytten av behandlingen opp imot hvor inngripende behandlingen er for den registrerte. I dette inngår risikoen for de registrertes rettigheter og friheter samt etterlevelse av forordningen herunder særskilt forordningens prinsipper og de registrertes rettigheter. Dette framgår av foregående kapittel om VURDERING AV RISIKOER OG TILTAK.

## Er behandlingsaktiviteten nødvendig?

|  |
| --- |
| **Er behandlingsaktivitetene nødvendig?** |
| Hvilken verdi/nytte har behandlingsaktiviteten for den behandlingsansvarlige?  |
|  |
| Hvilken verdi/nytte har behandlingsaktiviteten for den registrerte? |
|  |
| Hvilken verdi/nytte har behandlingsaktiviteten for samfunnet? |
|  |
| Hvilket eller hvilke rettslige grunnlag er behandlingen basert på og hvor tungt veier dette i forhold til vurdering av nødvendighet? |
|  |
| Er formålet i seg selv nødvending? |
|  |
| Kan behandlingen foretas på mindre inngripende måte?  |
|  |
| Foreligger andre forhold som er viktige i forhold til vurderingen av nødvendighet? |
|  |
| **Oppsummering - Hvor nødvendig vurderes behandlingsaktiviteten å være?**  |
|  |

## Hvor inngripende er behandlingsaktiviteten?

|  |
| --- |
| **Hvor inngripende er behandlingsaktiviteten?** |
| Oppleves innsamling av personopplysning som nærgående, sensitiv eller på annen måte inngripende? |
|  |
| Er dataene som behandles følsomme og/eller definert som særlige kategorier? |
|  |
| Er omfanget av behandlingen stor?Mange opplysninger om den enkelteOpplysninger om mangeStrekker behandlingen ut i tid og geografisk omfang |
|  |
| Tilgjengeliggjøres opplysningene for mange og eventuelt utenfor virksomheten? |
|  |
| Opptrer behandlingen i en sensitiv sammenheng? |
|  |
| Ansees prinsippene i personvernforordningen artikkel 5 som ivaretatt? |
|  |
| Er de registrertes rettigheter ivaretatt i behandlingen? |
|  |
| Foreligger restrisiko for de registrertes rettigheter og friheter som er utenfor akseptabelt risikonivå? |
|  |
| Kan behandlingen gjennomføres og formålet oppnås på en måte som er mindre inngripende og gir bedre vilkår for de registrerte? |
|  |
| Foreligger andre forhold som er viktige i forhold til vurderingen av nødvendighet? |
|  |
| **Oppsummering - Hvor inngripende vurderes behandlingsaktiviteten å være?** |
|  |

##  Er behandlingsaktiviteten proporsjonal og rimelig?

|  |
| --- |
| **Vurdering av behandlingsaktivitetens proporsjonalitet og rimelighet** |
| Er det et rimelig forhold mellom inngrepet som gjøres i personvernet og de fordelene som oppnås ved behandlingen?Baseres på vurderingen av hvor inngripende behandlingen er sett opp imot vurderingen av nødvendighet. Vurderingen kan kopieres til kapittel 1.  |
|  |

# Referanser

**Personopplysningsloven med personvernforordningen**

**Andre kilder**

* [Data protection impact assessments (ICO)](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/)
* [Data Protection Impact Assessment Template for Smart Grid and Smart metering systems](http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf)
* <https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/edpbartikkel29gruppen/Veileder-i-vurdering-av-personvernkonsekvenser-wp-248-norsk.pdf>
* ISO 29101 Privacy architecture framework

# Vedlegg

Vedlegg kan benyttes der det er hensiktsmessig for vurderingen.

Eksempler:

* Vurdering av behov for DPIA
* Risikovurdering(er)
* Beskrivelse av dataflyt – prosesskart
* Tiltaksplan
* Vurdering av rettslig grunnlag for behandlingen og eventuelt sekundært rettsgrunnlag
	+ Interesseavveining
	+ Samtykkeerklæring
* Personvernerklæring
* Personvernombudets uttalelse
* Registrertes uttalelse
* Ledelsens vurdering og konklusjon