PERSONVERNKONSEKVENSVURDERING



<Vurdering av>

Ansvar for behandlingen ligger til <avdeling>

Innhold

[1 INITIELL VURDERING AV BEHOV FOR PERSONVERNKONSEKVENSVURDERING 3](#_Toc85296371)

[1.1 Kort om den planlagte behandlingen av personopplysninger 3](#_Toc85296372)

[1.2 Roller og ansvar 3](#_Toc85296373)

[1.3 Omfanget av DPIAen 3](#_Toc85296374)

[1.4 Deltakere 4](#_Toc85296375)

[1.5 Vurdering av behov for DPIA 4](#_Toc85296376)

[2 FULLSTENDIG PERSONVERNKONSEKVENSVURDERING 8](#_Toc85296377)

[2.1 Systematisk beskrivelse 8](#_Toc85296378)

[2.2 Proporsjonalitet og formål 12](#_Toc85296379)

[2.3 De registrertes rettigheter 18](#_Toc85296380)

[3 Vurdering av personvernrisiko 22](#_Toc85296381)

[4 Planlagte tiltak for å håndtere risiko for de registrertes rettigheter 23](#_Toc85296382)

[5 Innspill og godkjenning 24](#_Toc85296383)

[5.1 De registrertes synspunkter 24](#_Toc85296384)

[5.2 Deltakerens anbefaling 24](#_Toc85296385)

[5.3 Kommentar fra personvernombudet 24](#_Toc85296386)

[5.4 Behandlingsansvarliges beslutning 26](#_Toc85296387)

[Vedlegg 27](#_Toc85296388)

**Versjonshåndtering**

|  |  |  |  |
| --- | --- | --- | --- |
| Versjon | Godkjent dato | Godkjent av | Kort beskrivelse av hva som er endret |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

[*Bruk av malen:   
- All tekst i* [ ] slettes ved ferdigstilling av dokumentet. Dette er ment som hjelpetekster.  
- All tekst i <>, skal fylles ut med tekst og gul markering fjernes før ferdigstilling.  
- Alle hjelpetekster i form av kommentarer slettes før ferdigstilling.]

[Nyttige referanser: [Datatilsynets veileder for vurdering av personvernkonsekvenser](https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/?id=7390), [Personopplysningsloven](https://lovdata.no/dokument/NL/lov/2018-06-15-38/*#*)]

# INITIELL VURDERING AV BEHOV FOR PERSONVERNKONSEKVENSVURDERING

|  |  |
| --- | --- |
|  | **Dersom det er sannsynlig at en behandling vil medføre høy risiko for fysiske personers rettigheter eller friheter skal den behandlingsansvarlige gjennomføre en vurdering av hvilke konsekvenser behandlingen vil ha for personopplysningsvernet før behandlingen kan starte. En vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer.**  **Gjennomfør initiell vurdering av behov for personvernkonsekvensvurdering. Ved to eller flere kryss skal fullstendig personvernkonsekvensvurdering gjennomføres. Les mer om hva de ulike vilkårene innebærer** [**her under (artikkel 29-gruppens kriterier for å vurdere behov for DPIA).**](https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-er-risiko-hoy/)[**Kommunen har også en egen oppgaveløser for DPIA**](https://allmenningen.bergen.kommune.no/ansatthjelpen/informasjonstjenester-og-ikt/personvern-og-informasjonssikkerhet/personvernkonsekvensvurdering-dpia) |

## Kort om den planlagte behandlingen av personopplysninger

[Før oppstart av alle tiltak som innebærer behandling av personopplysninger og ved større endringer av pågående tiltak, skal kommunen vurdere om tiltaket innebærer store risikoer for personvernet. Med tiltak menes nye tjenester, saksbehandlingsprosesser, IKT-løsninger, informasjonsaktiviteter, analyser av personopplysninger og andre aktiviteter som innebærer behandling av personopplysninger. Hvis behandlingen allerede er beskrevet i kommunens behandlingsprotokoll kan teksten herfra gjerne gjenbrukes.

Behandlingen er fra før beskrevet i kommunens behandlingsprotokoll.

Behandlingen er ikke beskrevet i kommunens behandlingsprotokoll. Behandlingsprotokollen må oppdateres før behandlingen starter.

<Sett inn tekst>

## Roller og ansvar

Den behandlingsansvarlige er den virksomhet eller person som bestemmer formålet med behandlinger av personopplysninger og hvordan behandlingen skal skje. Virksomheten som er behandlingsansvarlig for behandlingene av personopplysninger som skjer innenfor rammene av denne DPIAen er Voss herad ved avdeling for <Sett inn relevant avdeling>.

## Omfanget av DPIAen

Denne vurderingen av personvernkonsekvenser (DPIA) behandler følgende områder og tema:

[Beskriv hva dette dokumentet skal vurdere. Bruk gjerne punktlister]

<Sett inn tekst>

Denne vurderingen av personvernkonsekvenser (DPIA) vil ikke behandle følgende områder og tema:

[Beskriv hva som ikke vil bli behandlet i dette dokumentet. Begrunn hvorfor tema ikke er med. Bruk gjerne punktlister]

<Sett inn tekst>

## Deltakere

Følgende personer har deltatt i arbeidet med vurdering av behov for personvernkonsekvensvurdering/ fullstendig personvernkonsekvensvurdering:

|  |  |  |
| --- | --- | --- |
| **Navn** | **Rolle/stilling** | **Virksomhet** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Vurdering av behov for DPIA

Nedenfor følger en serie påstander om den planlagte behandlingen av personopplysninger. Avdelingen skal ta stilling til disse for å avgjøre om det er en plikt til å gjennomføre fullstendig personvernkonsekvensvurdering for den planlagte behandlingen.

[Nyttig referanse:   
[Når er det «høy risiko»? – Datatilsynet](https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-er-risiko-hoy/)  
[Når må man gjennomføre en vurdering av personvernkonsekvenser? - Datatilsynet](https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/)  
[Oppgaveløser om personvernkonsekvensvurdering (DPIA)](https://allmenningen.bergen.kommune.no/ansatthjelpen/informasjonstjenester-og-ikt/personvern-og-informasjonssikkerhet/personvernkonsekvensvurdering-dpia) ]

|  |  |  |  |
| --- | --- | --- | --- |
| # | Planlagt behandling innebærer | Vurdering | Begrunnelse |
| 1 | Systematisk monitorering eller overvåkning av innbyggere eller medarbeidere. Dette kan omfatte kameraovervåkning i stor skala av offentlig tilgjengelige områder, logging eller annen overvåkning av aktivitet på nett, logging av aktivitet på jobb eller innhenting av opplysninger fra sensorer eller lignende. | Ja  Nei |  |
| 2 | Behandling av personopplysninger for å evaluere læring, mestring og trivsel i skoler eller barnehager. | Ja  Nei |  |
| 3 | Kameraovervåking i skoler og barnehager i åpningstider. | Ja  Nei |  |
| 4 | Systematisk monitorering av effektivitet, ferdigheter, kunnskap, mental helse og utvikling. | Ja  Nei |  |
| 5 | Trening av kunstig intelligens ved bruk av særlige kategorier av personopplysninger eller svært personlige opplysninger i stor skala.  I dette tilfellet må behandlingen både inkludere særlige kategorier/svært personlige opplysninger OG behandlingen må være i stor skala OG behandlingen må skje i forbindelse med trening av kunstig intelligens. | Ja  Nei |  |
| 6 | Utvikling av tjenester for å forutsi økonomi, helse, preferanser, atferd eller lokasjon ved bruk av særlige kategorier av personopplysninger eller svært personlige opplysninger. | Ja  Nei |  |
| 7 | Innsamling av personopplysninger i stor skala gjennom «tingenes internett» eller velferdsteknologi. | Ja  Nei |  |

Dersom du svarte *ja* på minst en av påstandene ovenfor, skal du fylle ut en fullstendig personvernkonsekvensvurdering. Fortsett til del 2 – Fullstendig personvernkonsekvensvurdering.

Dersom du svarte *nei* på alle påstandene ovenfor, skal du fylle ut spørsmålene nedenfor.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Planlagt behandling innebærer | Vurdering | Begrunnelse |
| 8 | Innsamling av personopplysninger fra tredjepart. | Ja  Nei |  |
| 9 | Bruk av personopplysninger til evaluering og poengsetting | Ja  Nei |  |
| 10 | Automatiske beslutninger med rettslig eller tilsvarende betydelig virkning | Ja  Nei |  |
| 11 | Behandling av særlige kategorier av personopplysninger (inkludert biometriske og genetiske opplysninger) eller opplysninger av svært personlig karakter. | Ja  Nei |  |
| 12 | Personopplysninger behandles i stor skala. | Ja  Nei |  |
| 13 | Matching eller sammenstilling av datasett | Ja  Nei |  |
| 14 | Behandling av personopplysninger om sårbare registrerte | Ja  Nei |  |
| 15 | Innovativ anvendelse av ny teknologi eller organisatorisk løsning | Ja  Nei |  |
| 16 | Når behandlingen hindrer de registrerte å utøve en rettighet, eller gjøre bruk av en tjeneste eller en avtale. | Ja  Nei |  |
| 17 | Behandling av personopplysninger, uten samtykke, for vitenskapelige eller historiske formål. | Ja  Nei |  |
| 18 | Behandling av opplysninger om hvor den registrerte befinner seg (lokasjonsdata) | Ja  Nei |  |

Dersom du svarte ja på to eller flere påstander i tabellen ovenfor (nr. 8-18), skal du normalt gjennomføre en fullstendig personvernkonsekvensvurdering. For å avklare om den planlagte behandlingen er omfattet av unntak fra plikten til å gjennomføre DPIA, skal du besvare påstandene nedenfor.

|  |  |  |
| --- | --- | --- |
| Vilkår | Vurdering | Begrunnelse |
| Behandlingen er nødvendig for å oppfylle en rettslig forpliktelse eller skjer i forbindelse med utøvelse av offentlig myndighet. | Ja  Nei |  |
| Behandlingen har rettslig grunnlag i lovgivning som spesifikt regulerer den aktuelle behandlingen. | Ja  Nei |  |
| Det er allerede gjort en personvernkonsekvensvurdering av aktuelle lovgivningen som er dekkende for den planlagte behandlingen. | Ja  Nei |  |

Dersom du har svart ja på de tre påstandene ovenfor, er det likevel ikke nødvendig å gjennomføre en fullstendig DPIA.

Dersom du, basert på avhukede bokser, har kommet frem til at du skal gjennomføre en DPIA, skal dette gjøres. Har du, basert på avkrysningen av boksene, kommet til at det ikke skal gjennomføres en DPIA, men du likevel er usikker på om behandlingen kan innebære en høy risiko for personvernet skal:

* en fullstendig vurdering gjennomføres, eller
* personvernombudet kontaktes for råd.

|  |  |
| --- | --- |
| Behov for å gjennomføre fullstendig personvernkonsekvensvurdering | Ja  Nei |

# FULLSTENDIG PERSONVERNKONSEKVENSVURDERING

|  |  |
| --- | --- |
|  | ***På bakgrunn av initiell vurdering av behov for personvernkonsekvensvurdering er det sansynliggjort at planlagt behandling av personopplysninger vil innebære høy risiko for den/de registrertes rettigheter og friheter. Personvernkonsekvensvurdering gjennomføres derfor i tråd med krav etter personvernforordningen artikkel 35.*** |

## Systematisk beskrivelse

|  |  |
| --- | --- |
|  | ***Under følger en ren beskrivelse av planlagt behandlingsaktivitet og formål. Vurdering følger i del 4.2 og 4.3*** |

[Behandling av personopplysninger omfatter all bruk av personopplysninger, som innsamling, registrering, sammenstilling, lagring og utlevering - [Datatilsynets ordliste](https://www.datatilsynet.no/regelverk-og-verktoy/ordliste/)]

### Bakgrunn

[Beskrivelse av bakgrunnen for behandling av personopplysninger]

<Sett inn tekst>

### De planlagte behandlingsaktivitetene

Innhenting av personopplysninger fra den registrerte selv  
 Innhenting av personopplysninger fra andre kilder  
 Registrering   
 Strukturering   
 Lagring  
 Sammenstilling  
 Publisering  
 Profilering  
 Bearbeidelse  
 Analysering  
 Trening av kunstig intelligens eller maskinlæringsløsninger  
 Utlevering til tredjeparter  
 Sletting  
 Annet

[Gi en nærmere beskrivelse av de planlagte behandlingene av personopplysninger. Det er ikke nødvendig å gjenta det som allerede er beskrevet i avsnitt 1.1, men gi nærmere beskrivelse av de planlagte aktivitetene om dette er nødvendig for å gjennomføre ytterligere vurdering.]

<Sett inn tekst>

### Formål

Det/ de overordnede formålet/ formålene med behandlinger av personopplysninger som er omfattet av denne DPIA faller innenfor følgende hovedkategorier:

Administrasjon av kommunale ordninger eller tjenester  
 Gjennomføring av tjenester  
 Utvikling av tjenester  
 Forskning  
 Informasjonstiltak  
 Analyser for kvalitets-, styrings- og forbedringsformål  
 Administrasjon av egne ansatte  
 IT-sikkerhet  
 Fysisk sikkerhet  
 Annet

Mer spesifikt er formålet med behandlingen:

[Beskrivelse av formålet med behandling av personopplysninger]

<Sett inn tekst>

### Registrerte

De registrerte som vil omfattes av behandlingene som er beskrevet i denne DPIAen faller innenfor følgende hovedkategorier:

Innbyggere  
 Søkere om eller mottakere av tjenester  
 Kontaktperson i virksomhet  
 Ansatte  
 Barn  
 Elever   
 Barnehagebarn  
 Foresatte/forelder  
 Pasienter  
 Pårørende  
 Andre spesielt sårbare grupper  
 Besøkende på nettsider  
 Alle og enhver (for eksempel personer som filmes av overvåkningskameraer)  
 Andre - <Sett inn tekst>

Mer spesifikt vil det behandles følgende opplysninger om de registrerte:

[Beskrivelse av hvem det behandles personopplysninger om og relasjonen mellom dem og Voss herad]

<Sett inn tekst>

### Type og omfang

Personopplysningene som er relevante for behandlingene som er omfattet av denne DPIAen faller innenfor følgende hovedkategorier:

Identifisering og kontaktinformasjon, som navn, fødselsdato, adresse, e-postadresser og telefonnummer  
 Fødselsnummer  
 Opplysninger om innhold i en sak, som søknad, vurderinger og innhentede opplysninger  
 Opplysninger om innhold i et kundeforhold, som avtaler og opplysninger bruk av tjenester  
 Opplysninger om ansettelsesforhold, som stillingstittel, organisasjonsplassering, lønnsnivå, varsler, opplysninger i personalmappe.  
 Lokasjonsdata  
 Opplysninger fra sensorer eller overvåkningsutstyr  
 Opplysninger om rase eller etnisk opprinnelse (s)  
 Politisk oppfatning, religion, filosofisk overbevisning (s)  
 Fagforeningsmedlemskap (s)  
 Genetiske opplysninger (s)  
 Biometriske opplysninger (s)  
 Helseopplysninger (s)  
 Opplysninger om seksuelle forhold eller seksuell orientering (s)  
 Opplysninger om straffbare forhold og lovovertredelser (l)  
 Nettidentifikatorer, som IP-adresser  
 Annet - <Sett inn tekst>

Opplysninger merket med (s) betyr at opplysningstypen er særlige kategorier av personopplysninger. For disse kreves supplerende rettslig grunnlag, jf. avsnitt 2.2.1.3.

Opplysninger merket med (l) er opplysninger som er særregulert. Les mer om behandling av opplysninger om straffbare forhold og lovovertredelser i Personvernforordningen (GDPR) artikkel 10 og personopplysningsloven § 11.

Opplysningene er i strukturert form. Det vil si at opplysningene er organisert på en forhåndsdefinert måte og finnes i tabellform eller lignende.  
 Opplysningene er i ustrukturert form. Det vil si at opplysningene er uorganisert eller bare delvis organisert. Opplysningene finnes i fritekst i dokumenter, eller som bilder, film eller lydopptak.

Mer spesifikt vil det behandles følgende typer av personopplysninger:

[Beskrivelse av type og omfang av personopplysningene som behandles]

<Sett inn tekst>

### Datakilder

Opplysningene kommer fra den registrerte selv  
 Opplysningene kommer fra offentlige registre, som folkeregisteret  
 Opplysningene kommer fra andre registre

[Beskrivelse av datakilden for personopplysningene. Hvor kommer personopplysningene fra? For eksempel et eksternt/internt system?]

<Sett inn tekst>

### Lagring

Alle opplysninger lagres i system som driftes av Voss herad  
 Opplysninger lagres i leverandørens driftsmiljø eller i skytjeneste  
 Lagringen skjer utenfor EU/EØS-området

[Beskrivelse av lagringsmedium for personopplysningene.

Hvor lagres data/personopplysningene? Lokalt, hos leverandøren, i skyen? Kopieres personopplysningene i form av mellomlagring, backups eller lignende. Finnes det regelverk eller kriterier som styrer hvor lenge personopplysningene kan lagres?]

<Sett inn tekst>

### Tilgangskontroll

Det er utformet interne retningslinjer for styring av tilganger til personopplysninger  
 Tilgangsstyringen er basert på tjenstlig behov   
 Bruk av systemer og tilgang til personopplysninger i systemer logges  
 Vi har kontroll på hvem i kommunen, hos databehandler og hos eventuelle underleverandører som har tilgang til opplysningene

[Beskrivelse av hvem som har tilgang til personopplysningene. Det skal beskrives hvem i kommunen, hos databehandler og hvem hos eventuelle underleverandører som har tilgang til opplysningene. Hvordan tildeles og forvaltes disse tilgangene? Er det muligheter for rollestyrt/tjenestestyrt tilgang/autorisering? Kontrolleres det om personer har fått endret tillatelser/behov eller om de har sluttet eller byttet rolle? Loggføres tilgang til systemet? Loggføres endringer av data i systemet? Finnes det rutiner for å fjerne tilgang som ikke lenger er nødvendige? Hvordan følges tilganger opp?]

<Sett inn tekst>

### Prosessbeskrivelse – Dataflyt

[Beskrivelse av dataflyt og de overordnede prosessene som innebærer behandling av personopplysninger. Det oppfordres til å tegne eller lime inn allerede tegnede dataflyt (flytskjema). Beskriv hvilke systemer de flyter igjennom, hvor systemene ligger (sikker sone eller hos leverandør / sky).]

<Sett inn tekst>

### Eksterne mottakere

Ingen eksterne virksomheter mottar eller får tilgang til personopplysninger fra kommunen   
 Eksterne virksomheter mottar eller får tilgang til personopplysninger fra kommunen  
 Det er ikke inngått databehandleravtale med den eller de eksterne leverandørene  
 Det er inngått databehandleravtale med den eller de eksterne leverandørene  
 Det overføres ikke personopplysninger til land utenfor EU   
 Det overføres personopplysninger til land utenfor EU

[Beskrivelse av hvilke virksomheter det overføres personopplysninger til, om det er inngått databehandleravtale (eventuelt hvorfor ikke), på hvilke grunnlag personopplysninger overføres til land utenfor EU. Overføres personopplysninger til land utenfor EU skal det i tillegg beskrives på hvilke grunnlag og på hvilke måte dette gjøres, om det er gjennomført risikovurdering for dette samt hvilke overføringsmekanismer som brukes for overføringen.  
Mer informasjon:  
- <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overfore/>]

<Sett inn tekst>

### Innebygd personvern og personvern som standardinnstilling

Systemer/programvarer som blir brukt i behandlingen tilfredsstiller krav til innebygd personvern  
 Systemer/programvarer som blir brukt i behandlingen tilfredsstiller ikke krav til innebygd personvern  
 Systemer/programvarer som blir brukt i behandlingen har personvern som standardinnstilling  
 Det brukes ikke systemer/programvarer i behandlingen

[Beskrivelse av hva som er gjort for å ivareta personvernet i programvaren/systemet hvor personopplysninger behandles.]

<Sett inn tekst>

### Atferdsnormer/bransjenormer

Behandlingen etterlever relevant bransjenorm  
 Relevant bransjenorm eksisterer ikke  
 Det eksisterer en relevant bransjenorm, men behandlingen etterlever ikke denne

[Beskrivelse av atferdsnormer/bransjenormer som er relevante for behandlingen av personopplysninger. Referanse? Har vi vurdert om behandlingen følger disse? Dokumenter som viser etterlevelse av normen skal legges ved DPIAen]

<Sett inn tekst>

## Proporsjonalitet og formål

|  |  |
| --- | --- |
|  | **Under følger en vurdering av behandlingens nødvendighet og proporsjonalitet mellom behandling og formål** |

### Behandlingsgrunnlaget

[Både behandlingsgrunnlag i GDPR art. 6 og art.9, i tillegg til eventuelle supplerende rettslige grunnlag må oppgis i detalj.

Nyttige referanser:

[Artikkel 6. Behandlingens lovlighet](https://lovdata.no/lov/2018-06-15-38/gdpr/a6)

[Artikkel 9. Behandling av særlige kategorier av personopplysninger](https://lovdata.no/lov/2018-06-15-38/gdpr/a9)

[Datatilsynet – Veileder om behandlingsgrunnlag](https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/)

[Datatilsynet – Lovlighet, rettferdighet og gjennomsiktighet](https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/?id=7769)

[Kommunens oppgaveløser for valg av behandlingsgrunnlag](https://allmenningen.bergen.kommune.no/ansatthjelpen/informasjonstjenester-og-ikt/personvern-og-informasjonssikkerhet/valg-av-behandlingsgrunnlag) ]

Enhver behandling av personopplysninger må ha et rettslig grunnlag i personvernforordningen artikkel 6. Dersom det behandles særlige kategorier av personopplysninger skal det i tillegg foreligge et behandlingsgrunnlag i artikkel 9.

#### Behandlingsgrunnlag etter artikkel 6

Behandlingene som er beskrevet i denne DPIAen faller innenfor de rettslige grunnlagene som er beskrevet nedenfor. Velg ett av alternativene. Hvis du må velge to, beskriv hvilke deler av behandlingen som faller innenfor de ulike rettslige grunnlagene.

Samtykke, jf. personvernforordningen artikkel 6.1.a  
[Legg inn samtykketekst eller referanse til/ lenke til tekst eller stedet der samtykket skal hentes inn. Beskriv samtykkets innhold og hvordan samtykket skal hentes inn. Beskriv spesielt at samtykket er frivillig, spesifikt, informert og utvetydig.]

|  |  |  |
| --- | --- | --- |
| Et gyldig samtykke forutsetter at følgende vilkår er oppfylt – er samtykket: | | |
| frivillig? | Ja  Nei | [Begrunnelse, evt. henvisning] |
| spesifikt? | Ja  Nei | [Begrunnelse, evt. henvisning] |
| informert? | Ja  Nei | [Begrunnelse, evt. henvisning] |
| utvetydig? | Ja  Nei | [Begrunnelse, evt. henvisning] |
| gitt gjennom en aktiv handling? | Ja  Nei | [Begrunnelse, evt. henvisning] |
| dokumenterbart? | Ja  Nei | [Begrunnelse, evt. henvisning] |
| mulig å trekke tilbake like lett som det ble gitt? | Ja  Nei | [Begrunnelse, evt. henvisning] |

[Om det rettslige grunnlaget ikke er samtykke, så kan tabellen slettes.]

<Sett inn tekst>

Avtale med den registrerte, jf. personvernforordningen artikkel 6.1.b  
[Legg inn referanse til/ lenke til relevante typer av avtale. Redegjør også for hvorfor behandlingen av personopplysninger er nødvendig for å oppfylle avtalen.]

<Sett inn tekst>

Rettslig forpliktelse, jf. personvernforordningen artikkel 6.1.c  
[Legg inn referanse til lov, forskrift eller annen rettslig forpliktelse som hjemler behandlingen. Redegjør også for hvorfor behandling av personopplysninger er nødvendig for å oppfylle den rettslige forpliktelsen. Husk at i de tilfeller der kommunen har en lovmessig forpliktelse til å gjennomføre offentlig myndighet, skal hjemles i artikkel 6.1.e]

<Sett inn tekst>

Vitale interesser, jf. personvernforordningen artikkel 6.1.d  
[Beskriv de vitale interessene som gjør seg gjeldende for behandlingen.]

<Sett inn tekst>

Allmennhetens oppgave og utøvelse av offentlig myndighet, jf. personvernforordningen artikkel 6.1.3  
[Legg inn referanse til lov eller forskrift som beskriver oppgaven eller den offentlige myndigheten. Redegjør også for hvorfor behandling av personopplysninger er nødvendig for å utøve den offentlige myndigheten slik det er beskrevet i lov eller forskrift.]

<Sett inn tekst>

Berettiget interesse (interesseavveining), jf. personvernforordningen artikkel 6.1.f  
[Legg inn interesseavveining og balansetest som dokumenterer de berettigede interessene eller referanse til/ lenke til interesseavveiningen]

<Sett inn tekst>

#### Videre bruk til forenlig formål

Den behandlingsansvarlige anser det som nødvendig å behandle personopplysninger for annet formål enn det som personopplysningene er blitt samlet inn for.

Behandlingene har ikke sitt rettslige grunnlag i den registrertes samtykke  
 Behandlingene har ikke sitt rettslige grunnlag i lov eller forskrift  
 Personopplysninger skal ikke behandles videre for andre formål

Forenlighetsvurdering:

[Dersom relevant: Beskrivelse av forbindelsen mellom formålet som personopplysningene er blitt samlet inn for, og formålene med den tiltenkte viderebehandlingen. Følgende momenter skal beskrives:

* Sammenhengen personopplysningene ble samlet inn i og forholdet mellom de registrerte og den behandlingsansvarlige
* Personopplysningenes art og spesielt beskrivelse av behandlingen av særlige kategorier av personopplysninger og opplysninger om straffedommer og lovovertredelser
* Mulige konsekvenser av den videre behandlingen for de registrerte
* Planlagte garantier for de registrerte, som kryptering eller pseudonymisering]

<Sett inn tekst>

Den behandlingsansvarlige har gjort en helhetlig vurdering av behandlingen, og anser vilkårene for viderebehandling for forenlig formål som oppfylt.

#### Behandlingsgrunnlaget etter artikkel 9

Dersom aktiviteten(e) som omfattes av denne personvernkonsekvensvurderingen innebærer behandling av helseopplysninger, fagforeningsopplysninger med mer (se avsnitt 2.1.5), så må ett av vilkårene i artikkel 9 oppfylles. Dette kommer i tillegg til oppfyllelse av ett av vilkårene i artikkel 6. Behandlingene av særlige kategorier av personopplysninger som er beskrevet i denne DPIAen faller innenfor følgende rettslige grunnlag:

Behandling basert på samtykke, jf. personvernforordningen artikkel 9.2.a

|  |  |  |
| --- | --- | --- |
| Et gyldig samtykke forutsetter at følgende vilkår er oppfylt – er samtykket: | | |
| Eksplisitt | Ja  Nei | [Begrunnelse, evt. henvisning] |

[Legg inn samtykketekst eller referanse til/ lenke til tekst eller stedet der samtykket skal hentes inn. Beskriv samtykkets innhold og hvordan samtykket skal hentes inn. Beskriv spesielt at samtykket er frivillig, spesifikt, informert og utvetydig. Vis til gjennomgangen av vilkår for samtykke i avsnitt 2.2.1.1. Dersom behandlingen ikke er basert på samtykke, kan boksen over slettes]

<Sett inn tekst>

Behandlinger på arbeidsrettens, trygderettens og sosialrettens områder, jf. personvernforordningen artikkel 9.2.b  
[Legg inn referanse til lov eller forskrift som hjemler behandlingen (primært folketrygdloven og sosialtjenesteloven). Redegjør også for hvorfor behandling av personopplysninger er nødvendig for å oppfylle lov eller forskrift.]

<Sett inn tekst>

Vitale interesser, jf. personvernforordningen artikkel 9.2.c  
[Legg inn redegjørelse for de registrertes vitale interesser og for hvorfor samtykke eller andre rettslige grunnlag ikke er aktuelle eller referanse til/ lenke til slik vurdering.]

<Sett inn tekst>

Opplysninger av politisk, religiøs eller fagforeningsmessig art utført av organisasjon eller stiftelse, jf. personvernforordningen artikkel 9.2.d  
[Legg inn organisasjonsnummer og formål med den ideelle sammenslutningen, stiftelsen eller organisasjonen som er behandlingsansvarlig for behandlingen og redegjør for nødvendigheten av å behandle særlige kategorier av personopplysninger.]

<Sett inn tekst>

Opplysninger den registrerte har gjort offentlig kjent, jf. personvernforordningen artikkel 9.2.e  
[Redegjør for hvor den registrerte har gjort særlige kategorier offentlig kjent og for hvorfor videre behandling av opplysningene er nødvendig.]

<Sett inn tekst>

Fastsette, gjøre gjeldende eller forsvare et rettskrav, jf. personvernforordningen artikkel 9.2.f  
[Redegjør for relevante rettskrav og hvorfor behandling av særlige kategorier av personopplysninger er nødvendige for å fastsette, gjøre gjeldende eller forsvare rettskravet.]

<Sett inn tekst>

Viktige allmenne interesser, jf. personvernforordningen artikkel 9.2.g  
[Legg inn referanse til lov eller forskrift som hjemler behandlingen. Redegjør for hvorfor behandling av personopplysninger er nødvendig for å oppfylle lov eller forskrift og for hvorfor behandlingen anses som forholdsmessig.]

<Sett inn tekst>

Yting av helsetjenester, jf. personvernforordningen artikkel 9.2.h  
[Legg inn referanse til lov eller forskrift som hjemler behandling av særlige kategorier av personopplysninger til formål knyttet til yting av helsetjenester.]

<Sett inn tekst>

Allmenne folkehelsehensyn, jf. personvernforordningen artikkel 9.2.i  
[Legg inn referanse til lov eller forskrift som hjemler behandling av særlige kategorier av personopplysninger til formål knyttet til allmenne folkehelsehensyn.]

<Sett inn tekst>

Arkiv, forskning og statistikk, jf. personvernforordningen artikkel 9.2.j  
[Legg inn referanse til lov eller forskrift som hjemler behandling av særlige kategorier av personopplysninger til arkiv-, forsknings, og statistikkformål.]

<Sett inn tekst>

Det behandles ikke særlige kategorier av personopplysninger

### Formålsbegrensning og Dataminimering

Personopplysninger skal kun behandles for å oppfylle spesifikke, uttrykkelig angitte og berettigede formål. Dataminimering innebærer at personopplysninger som ikke er nødvendige for å oppfylle formålet ikke skal behandles.

[Nyttig referanse:

[Datatilsynets personvernprinsipper – Formålsbegrensning](https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/formalsbegrensning/)

[Datatilsynets personvernprinsipper - Dataminimering](https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/dataminimering/)]

☐ Formålet eller formålene klart definert   
☐ Formålet nedfelt i forskrift eller lov  
☐ Behandlingen har et kontrollformål (for eksempel kontroll innen skatt, NAV eller kontroll av arbeidsgivere)  
☐ Er det noe i egen forskrift eller andre forskrifter eller lover som begrenser formålet?  
☐ Er formålet beskrevet i løsning, tjeneste eller system utfordrende sett opp mot rettsgrunnlaget  
☐ Omfatter rettslig grunnlag både egne formål og utlevering?   
☐ Er formålet definert slik at det samsvarer med forventningene de registrerte kan ha ut fra egen forskrift, lov eller samtykkevilkår?

[Beskrivelse av hvordan det jobbes for å sikre formålsbegrensning og dataminimering]

<Sett inn tekst>

|  |  |  |
| --- | --- | --- |
|  | Vurdering | Begrunnelse |
| Er samtlige personopplysninger som behandles nødvendige for å nå formålet? | Ja  Nei |  |
| Er dette den minste inngripende måten å oppnå formålet på? | Ja  Nei |  |
| Kan samme formål oppnås ved en mer begrenset innsamling av personopplysninger? | Ja  Nei |  |
| Kan formålet oppnås ved pseudonymiserte eller anonymiserte personopplysninger? | Ja  Nei |  |

### Riktighet

Personopplysninger skal være korrekte og oppdaterte nok sett opp mot formålet med behandlingen.

[Nyttig referanse: [Datatilsynets personvernprinsipper – Riktighet](https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/?id=7772)]

☐ Det er gjort en vurdering av behovet for hvor ofte personopplysninger må oppdateres, f.eks. mot offentlige registre.  
☐ Det er gjort en vurdering av behov for validering og kontroll av personopplysninger som registreres av den registrerte selv.

[Beskrivelse av hvordan det jobbes for å sikre riktighet]

<Sett inn tekst>

### Lagringsbegrensning

Personopplysninger skal slettes når formålet med behandlingene av personopplysninger er oppfylt og det ikke fins plikter til å oppbevare opplysningene.

Det er utformet retningslinjer for oppbevaring og sletting  
 Det er utformet systemstøtte for sletting  
 Det er ikke tatt stilling til oppbevaring og sletting av personopplysninger

[Beskrivelse av hvor lenge vi skal behandle personopplysningene for å oppnå formålet, og eventuelle planlagte frister for sletting eller avsluttet behandling. Vurder hver enkelt type personopplysning og ulike lagringssteder.]

<Sett inn tekst>

[Nyttig referanse: [Datatilsynets personvernprinsipper – Lagringsbegrensning](https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/?id=7773)]

### Egnet sikkerhetsnivå

|  |  |
| --- | --- |
|  | **Ved vurderingen av egnet sikkerhetsnivå skal det tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.** |

|  |  |
| --- | --- |
| **Er det gjennomført risikovurdering av løsningen?** | Ja  Nei |
| Dersom ja: |  |

|  |  |  |
| --- | --- | --- |
|  | Vurdering | Begrunnelse |
| Er nødvendige sikkerhetstiltak for å sikre tilstrekkelig konfidensialitet, integritet og tilgjengelighet ved behandlingen implementert og iverksatt? | Ja  Nei |  |
| Er løsningen tilstrekkelig robust til å takle ytre påvirkning (hacking)? | Ja  Nei |  |
| Er løsningen robust nok til å takle indre påvirkning (oppskalering av innhold, brukere og integrasjoner) ? | Ja  Nei |  |
| Er restrisiko håndterbar og akseptabel? | Ja  Nei |  |

|  |  |
| --- | --- |
| Risikorapport-ID i sak og arkivsystem: <Sett inn tekst> Dato ferdigstilt: <Sett inn tekst> |  |

|  |  |
| --- | --- |
|  | **Ved valg av tiltak skal det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter.** |

[Redegjør for sikkerhetstiltakene som er/skal iverksettes for å beskytte personopplysningene (eks. Taushetserklæringer, databehandleravtaler, atferds-/bransjenormer, tilgangsstyring, rutiner for å følge opp eventuelle underleverandørers etterlevelse av databehandleravtale og andre tiltak]

<Sett inn tekst>

## De registrertes rettigheter

### Rettigheter etter personopplysningsregelverket:

[Nyttig referanse: [Datatilsynet – Den registrertes rettigheter](https://www.datatilsynet.no/rettigheter-og-plikter/den-registrertes-rettigheter/)]

#### Hvordan ivaretas de registrertes rett til informasjon

Informasjon om behandlingen av personopplysninger er gitt i virksomhetens personvernerklæring.

Informasjon er gitt til den registrerte i forbindelse med avgivelse av samtykke.

Informasjon er gitt til den registrerte i forbindelse med inngåelse av avtale.

Informasjon er gitt til den registrerte i forbindelse med påbegynt søknad eller leveranse av offentlig tjeneste.

Informasjon er gitt til den registrerte i annen sammenheng.

Informasjonen antas å være forutsigbar for de registrerte.

Det er ikke etablert planer og rutiner for å gi informasjon til den registrerte om behandlingen.

[Beskriv sammenhengen til informasjonen som er gitt. Link til personvernerklæring eller andre informasjonskilder.]

<Sett inn tekst>

#### Hvordan ivaretas de registrertes rett til innsyn?

Den registrerte er gitt informasjon om innsyn i egne personopplysninger på personvernerklæring og i andre passende kanaler.

Virksomheten har utformet løsning eller kanal for å bestille innsyn i egne personopplysninger.

Virksomheten har utformet rutiner for å hente ut personopplysninger, verifisere at den som har henvendt seg med ønske om innsyn faktisk er den registrerte og for sikker utsendelse av opplysningene.

Det er ikke etablert planer og rutiner for å gjennomføre den registrertes rett til innsyn.

[Beskriv hvordan den registrertes rett til innsyn kan oppfylles.]

<Sett inn tekst>

#### Hvordan ivaretas de registrertes rett til sletting og retting?

Virksomheten har utformet rutiner for å rette feilaktige personopplysninger ved henvendelse fra den registrerte.

Den registrerte er gitt informasjon om muligheten til å få slettet personopplysninger om seg selv på personvernerklæring og i andre passende kanaler.

Virksomheten har utformet rutiner for å slette personopplysninger ved henvendelse fra den registrerte.

Det er ikke etablert planer og rutiner for å gjennomføre den registrertes rett til sletting og retting.

[Gi en nærmere beskrivelse av rutiner for sletting og retting av de registrertes opplysninger. Finnes det dokumenterte rutiner for retting og sletting? Dersom den registrerte ikke selv kan rette feil i egne personopplysninger, finnes det andre måter å gjøre det på? Gis det informasjon til den registrerte om muligheten til å slette opplysningene og om hvordan slettingen kan gjøres? Finnes det rettslig grunnlag for å nekte sletting? Hvis ja, hjemmel?]

<Sett inn tekst>

#### Hvordan ivaretas de registrertes rett til begrensning av behandlingen?

Virksomheten informerer den registrerte om retten til å begrense behandlingen.

Virksomheten har rutiner for å gjennomføre begrensning.

Det er ikke etablert planer og rutiner for å gjennomføre den registrertes rett til begrensning av behandling.

[Beskriv hvordan den registrertes rett til begrensning kan oppfylles.]

<Sett inn tekst>

#### Hvordan ivaretas de registrertes rett til å protestere mot en behandling?

Virksomheten informerer den registrerte om retten til å protestere på en behandling.

Virksomheten har rutiner for å håndtere en protest mot en behandling.

Det er ikke etablert planer og rutiner for å gjennomføre den registrertes rett til å protestere mot en behandling.

[Beskriv hvordan den registrertes rett til å protestere kan oppfylles.]

<Sett inn tekst>

#### Hvordan ivaretas de registrertes rettigheter til dataportabilitet?

☐ Virksomheten informerer den registrerte om retten til dataportabilitet.

☐ Virksomheten har rutiner for å håndtere en forespørsel om dataportabilitet.

☐ Det er ikke etablert planer og rutiner for å gjennomføre den registrertes rett til dataportabilitet.

☐ Ikke relevant

[Beskriv hvordan den registrertes rett til dataportabilitet kan oppfylles.]

<Sett inn tekst>

#### Hvordan håndheves forbud mot automatiserte individuelle avgjørelser?

Virksomheten informerer den registrerte om retten til å ikke være gjenstand for automatiserte individuelle avgjørelser og profilering.

Virksomheten har rutiner for å sikre at personopplysninger kun behandles til automatiserte avgjørelser og profilering om det fins et gyldig rettslig grunnlag for dette.

Det er ikke etablert planer og rutiner for å håndheve forbudet mot automatiserte individuelle avgjørelser.

Ikke relevant.

[Beskriv hvordan forbudet mot automatiserte individuelle avgjørelser håndheves]

<Sett inn tekst>

#### Øvrige rettigheter og friheter som er relevant for behandlingen:

Behandlingen kan ha konsekvenser for

Den registrertes rett til privatliv

Den registrertes rett til kommunikasjonsvern

Den registrertes rett til ytringsfrihet

Den registrertes rett til tanke-, tros- og religionsfrihet

Den registrertes rett til å ikke bli diskriminert

Barns rettigheter etter barnekonvensjonen

Andre rettigheter

[Hvis virksomheten har krysset av på noen av punktene ovenfor, redegjør for hvilke rettigheter og friheter som kan være truet av behandlingen. Det kan også være andre rettigheter som blir truet, og i slike tilfeller skal det redegjøres for disse. Det er ikke nødvendig å vurdere risiko eller foreslå tiltak nå. Alle trusler eller utfordringer mot de registrertes rettigheter og friheter, inkludert personverntrusler, skal være en del av risikovurderingen i 3.]

<Sett inn tekst>

# 

# Vurdering av personvernrisiko

|  |  |
| --- | --- |
|  | **Under følger en vurdering av risikoen behandlingen innebærer for de registrertes rettigheter og friheter etter personopplysningsloven og EMK.** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Personvernrisiko** | **Beskrivelse av risikoen** | **Risikoens alvorlighetsgrad**  (Høy/ middels/ lav) | **Forslag til risikoreduserende tiltak** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |

[Dersom det er gjennomført ROS av en IKT-løsning som har berøringspunkter mot denne personvernkonsekvensvurderinger, bør det vurderes å inkludere en oppsummering av de mest relevante risikoer i dette avsnittet.]

<Sett inn tekst>

Ved personvernrisikoer som vurderes som middels eller høy skal det vurderes å gjennomføre risikoreduserende tiltak.

# Planlagte tiltak for å håndtere risiko for de registrertes rettigheter

|  |  |
| --- | --- |
|  | **Under følger en beskrivelse av hvilke tiltak en planlegger å iverksette for å håndtere risiko for de registrertes og andre berørte personers rettigheter beskrevet i avsnitt 3. Hvem som er ansvarlig for tiltakene og tidspunktet disse skal implementeres må gå frem av beskrivelsen under.** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nr.** | **Personvernrisiko** | **Risikoreduserende tiltak** | **Ansvarlig for tiltak** | **Frist for tiltak** | **Vurdering av risiko etter tiltak**  (Høy/ middels/ lav) |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

[Dersom det er gjennomført ROS av en IKT-løsning som har berøringspunkter mot denne personvernkonsekvensvurderinger, bør det vurderes å inkludere en oppsummering av de mest relevante tiltakene i dette avsnittet.]

<Sett inn tekst>

# Innspill og godkjenning

## De registrertes synspunkter

De registrertes synpunkter er innhentet.

De registrertes synspunkter er ikke innhentet

[Beskriv hvordan de registrertes synspunkter er innhentet og hovedpunktene i de registrertes synspunkter. Dersom de registrertes synspunkter ikke er innhentet, beskriv hvorfor.]

<Sett inn tekst>

## Deltakerens anbefaling

|  |  |
| --- | --- |
|  | **Under følger prosjektets samlede vurdering av personvernet og anbefaling til den behandlingsansvarlige.** |

[Forslag:   
Ved å implementere de planlagte tiltakene, er deltakerne i denne personvernkonsekvensvurderingen av den oppfatning at personvernrisikoen er redusert i tilstrekkelig grad til at behandlingen kan gjennomføres i tråd med personvernforordningen, uten forhåndsdrøftelse med Datatilsynet.   
  
Behandlingsansvarlig avgjør hvorvidt personvernkonsekvensvurderingen er tilstrekkelig utført og om personvernrisikoen er på et akseptabelt nivå.]

<Sett inn tekst>

## Kommentar fra personvernombudet

|  |  |
| --- | --- |
|  | **I tråd med Art. 35 (2) har den behandlingsansvarlige rådført seg med personvernombudet i forbindelse med utførelsen av personvernkonsekvensvurdering**. |

Personvernombudet har vurdert om behandlingen av personopplysninger som er beskrevet i denne DPIAen tilfredsstiller de krav som oppstilles i personvernlovgivningen.

Alternativ 1:

Personvernombudet vurderer at de tiltak (herunder: personvernøkende tiltak, sikkerhetstiltak, rutiner, informasjonsskriv og opplæring, mv.) som er beskrevet i denne personvernkonsekvensvurderingen, må ferdigstilles og operasjonaliseres.

[Skriv inn eventuelle vurderinger av de enkelte tiltak] – <Sett inn tekst>

Totalt sett er de planlagte tiltakene for å håndtere risikoene, herunder garantier, sikkerhetstiltak og mekanismer for å sikre vern av personopplysninger og for å påvise at forordning overholdes, idet det tas hensyn til de registrertes og andre berørte personers rettigheter og berettigede interesser, vurdert til å være innfridd basert på ovennevnte informasjon.

Det vurderes at behandlingen med de risikoreduserende tiltak som er omtalt over, ikke innebærer høy restrisiko, slik at det ikke er nødvendig å konsultere Datatilsynet. Behandlingen kan aksepteres dersom tiltakene blir implementert og fulgt opp.

Alternativ 2:

De tiltak (herunder: personvernøkende tiltak, sikkerhetstiltak, rutiner, informasjonsskriv og opplæring, mv.) som er beskrevet i denne personvernkonsekvensvurderingen, anses ikke til å i tilstrekkelig grad redusere risikoen for de registrertes personvern.

[Skriv inn argumenter for og imot å akseptere behandlingen] – <Sett inn tekst>

Personvernombudet anser risikoen for de registrerte ved behandlingen som for høy til at behandlingen bør gjennomføres som planlagt til tross av for de planlagte tiltakene. Det anbefales derfor at tiltaket ikke gjennomføres uten at behandlingen av personopplysninger endres grunnleggende eller at ytterligere risikoreduserende tiltak implementeres.  
  
Dersom den behandlingsansvarlige likevel velger å gjennomføre behandlingen, anbefaler personvernombudet at Datatilsynet kontaktes for å gjennomføre den lovpålagte forhåndskonsultasjonen.

Alternativ 3:

<Sett inn egentilpasset vurdering>

## Behandlingsansvarliges beslutning

|  |  |
| --- | --- |
|  | **Behandlingsansvarlig avgjør om personvernkonsekvensvurderingen er tilfredsstillende utført og om personvernrisikoen er redusert til akseptabelt risikonivå eller om forhåndsdrøfting med Datatilsynet er nødvendig før behandlingen kan iverksettes. Behandlingsansvarlig skal rådføre seg med personvernombudet.** |

Del 1:

Personvernombudets råd følges

Personvernombudets råd settes til side

Del 2:

Voss herad ved behandlingsansvarlige kommunal-/ stabssjef vurderer det slik at man ved å følge planlagte tiltak som fremgår av denne personvernkonsekvensvurdering reduserer personvernrisikoen til et akseptabelt risikonivå. Behandling kan gjennomføres i samsvar med personvernforordningen, uten forhåndsdrøfting med Datatilsynet.

Voss herad ved behandlingsansvarlige kommunal-/ stabssjef vurderer det slik at planlagte tiltak ikke reduserer personvernrisikoen tilstrekkelig. Forhåndsdrøfting med Datatilsynet er nødvendig før eventuell behandling kan starte.

Voss herad ved behandlingsansvarlige kommunal-/ stabssjef vurderer det slik at behandlingen ikke kan gjennomføres som forespeilet i denne personvernkonsekvensvurdering.

<Sett inn eventuell utfyllende tekst>

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| Godkjent av |  |  | Dato |

# Vedlegg

|  |  |
| --- | --- |
| **Temaer for diskusjon i risikovurdering** | |
|  |  |
| Risikomomentene nedenfor er gruppert ut fra personvernprinsippene i personvernforordningen artikkel 5. I tillegg er risikoer knyttet til kontroll med underleverandører lagt til som egen gruppe. Ved gjennomføring av DPIAer kan bør alle prinsippene behandles, men de antatt mest relevante risikomomentene skal vurderes konkret. | |
|  |  |
| **Tema** | **Personvernrisiko** |
| **A. Lovlighet, rettferdighet, åpenhet** | |
| Personopplysninger behandles uten dekkende rettslig grunnlag | Sammenstilling av opplysninger (spesielt særlige kategorier) uten rettslig grunnlag. |
| Oppslag/ rapport/ uttrekk uten rettslig grunnlag |
| Når behandlingsgrunnlaget er samtykke: vilkårene for samtykke er ikke oppfylt på grunn av feil ved innhenting. |
| Når behandlingsgrunnlaget er utøvelse av offentlig myndighet: Den rettslige reguleringen av tiltaket er ikke tilstrekkelig klar slik at den registrerte kan forutse at behandlingen vil skje. |
| Innsamlede personopplysninger benyttes til annet enn fastsatt formål (formålsutglidning) | Bruk av fritekstfelt fører til mangel på kontroll ved innhenting av personopplysninger |
| Manglende interne rutiner som begrenser hva innsamlede personopplysninger kan behandles. |
| Manglende åpenhet | Det gis ikke tilstrekkelig informasjon til de registrerte om behandlingen av personopplysninger |
| Informasjon om behandling er ikke tilstrekkelig tilpasset målgruppen |
| Innbygger/ansatte får ikke tilstrekkelig informasjon til å gjøre et informert valg |
| Bruk av personopplysninger til profilering er ikke gjort kjent/ skjer ikke på en tilstrekkelig åpen måte |
| Personopplysninger behandles på en ikke rettferdig måte | Det unnlates å gi informasjon som vil kunne være avgjørende for om den registrerte ønsker å benytte seg av et tilbud eller tjeneste |
| De registrertes rettigheter blir ikke tilstrekkelig ivaretatt | Innbyggere/ansatte får ikke innsyn i personopplysninger om seg selv |
| Det er ikke etablert løsning for dataportabilitet |
| Innbyggere/ansatte får ikke mulighet å motsette seg profilering |
| Innbyggere/ansatte får ikke mulighet å motsette seg automatisert behandling |
| **B. Formålsbegrensning** | |
| Behandlingen mangler legitimt og klart formål | Det er ikke definert et tydelig formål med en behandling i behandlingsprotokollen |
| Behandlingen er ikke nødvendig eller proporsjonal for formålet | Det er ikke gjort en vurdering av nødvendighet eller proporsjonaliteten ved behandlingen |
| **C. Dataminimering** | |
| Det samles inn mer personopplysninger enn det som er nødvendig for formålet | Innsamling av personopplysninger følger ikke en etablert, skriftlig rutine for å begrense innsamlingen. |
| Overskuddsinformasjon slettes ikke |
| **D. Riktighet** | |
| Personopplysningene som behandles er ikke korrekte | Det mangler rutiner for å sikre korrekte opplysninger |
| Det mangler rutiner for å sikre oppdatering av opplysninger mot autoritative kilder (som folkeregisteret) |
| Innbyggere/ansatte får ikke korrigert sine personopplysninger |
| **E. Lagringsbegrensning** | |
| Retten til å bli glemt etterleves ikke. | Innbyggere/ansatte får ikke slettet sine personopplysninger ved hevendelse |
| Personopplysninger lagres lengre enn det som er nødvendig for formålet | Det er ikke etablert sletterutiner. |
| Sletterutinene fører til lagring lengre enn formålet krever. |
| **F. Informasjonssikkerhet** | |
| Manglende risikovurdering av informasjonssikkerhet | Ingen etablert rutine for gjennomføring av risikovurderinger/ ROS |
| Mangelfull konfidensialitet | Misbruk av personopplysninger, snoking, identitetstyveri mv. |
| Eksponering av særlig sårbare personer, som barn, umyndiggjorte eller trusselutsatte (kode 6 eller 7) |
| Mangelfull tilgangsstyring |
| Manglende endringer/avslutning av tilganger |
| Transport av personopplysninger på usikker kanal |
| Lagring av personopplysninger usikkert å lagringssted |
| Mangelfull integritetskontroll | Manglende rutiner for oppdatering og endring av opplysninger |
| Mangelfull tilgjengelighet | Manglende krav til tilgjengelighet |
| **G. Ansvarlighet** | |
| Mangelfull dokumentasjon | Dokumentasjon av behandlinger av personopplysninger i rutiner og prosedyrer er mangelfull. |
| Manglende internkontroll | Behandlingsansvarlige har ikke etablert effektive og dokumenterte tiltak for å sikre at personvernlovgivningen etterleves. |
| Manglende styrende tiltak, som policyer og retningslinjer for behandling av personopplysninger, samt manglende beslutninger om risikoakseptanse |
| Manglende gjennomførende tiltak, som rutiner og veiledning i fagsystemer. |
| Manglende kontrollerende tiltak, som revisjoner og stikkprøvebaserte kontroller. |
| **H. Kontroll med underleverandører** | |
| Mangelfull kontroll med databehandlere | Utilstrekkelige databehandleravtaler |
| Utilstrekkelig kontroll og revisjon av databehandleres behandlinger |
| Overføring av persnoopplysninger til tredjestat | Utilstrekkelig grunnlag for overføring av personopplysninger til tredjeland |
| **I. Rettigheter** | |
| Brudd / manglende oppfyllelse av rettigheter | Behandlingen kan resultere i diskriminering |
| Behandlingen begrenser ytringsfrihet og religionsfrihet |
| Behandlingen kan resultere i at pasienter og brukere ikke får oppfylt sine rettigheter etter pasient- og brukerrettighetsloven |
| Behandlingen kan resultere i at barns rettigheter etter barnekonvensjonen ikke blir fulgt |
| Behandlingen kan resultere i brudd på andre rettigheter innbyggere har med hjemmel i lov. |