Vurdering av
personvernkonsekvenser (PVK)

PVK KOMMUNE MAL

*<Tittel på den spesifikke endringen/utviklingen>*

*Status og dato (xx.xx.xxxx) (velg mellom under arbeid/ oppdatert/ godkjent/ ferdig):*



*Malversjon 1.0*

Innhold

[2 Om vurdering av personvernkonsekvenser 2](#_Toc25338381)

[2.1 Hva er en vurdering av personvernkonsekvenser? 2](#_Toc25338382)

[2.2 Når skal en vurdering av personvernkonsekvenser gjennomføres? 2](#_Toc25338383)

[2.3 Hvordan skal en vurdering av personvernkonsekvenser gjennomføres? 2](#_Toc25338384)

[3 Planlegge og organisere (trinn 1) 3](#_Toc25338385)

[3.1 Behandlingsansvarlig 3](#_Toc25338386)

[3.2 Registrertes representanter 3](#_Toc25338387)

[3.3 Hvordan involvere personvernombudet 3](#_Toc25338388)

[3.4 Bakgrunn 3](#_Toc25338389)

[3.5 Deltakelse i vurderingen 4](#_Toc25338390)

[3.6 Endringslogg 4](#_Toc25338391)

[4 Dokumentasjon av behandlingen (trinn 2) 4](#_Toc25338392)

[4.1 Matrise 5](#_Toc25338393)

[4.2 Risikovurdering av informasjonssikkerheten 8](#_Toc25338394)

[5 Vurdering av personvernkonsekvenser for den enkelte (trinn 3) 9](#_Toc25338395)

[5.1 Vurdering av personvernkonsekvenser 0](#_Toc25338396)

[5.2 Tiltak for å redusere risiko 0](#_Toc25338397)

[5.3 Vurderinger 0](#_Toc25338398)

[6 Avslutning og endelig vurdering (trinn 4) 1](#_Toc25338399)

[6.1 Behandlingsansvarliges vurdering 1](#_Toc25338400)

[6.2 De registrertes (representant) sin vurdering 1](#_Toc25338401)

[6.3 Vurdering og råd fra personvernombudet 1](#_Toc25338402)

[6.4 Endringer etter vurderingen av personvernombudet 2](#_Toc25338403)

[6.5 Behov for forhåndsdrøftelse med Datatilsynet 2](#_Toc25338404)

[6.6 Endelig godkjenning 3](#_Toc25338405)

[7 Vedlegg 4](#_Toc25338406)

[7.1 Konsekvenskategorier og konsekvensområder 4](#_Toc25338407)

[7.2 Eksempler på scenarioer 5](#_Toc25338408)

# Om vurdering av personvernkonsekvenser

## Hva er en vurdering av personvernkonsekvenser?

En vurdering av personvernkonsekvenser (PVK, på engelsk: Data Protection Impact Assessment – DPIA) skal sikre at personvernet til personene kommunen behandler og registrerer personopplysninger om blir ivaretatt. Vurderingen av personvernkonsekvenser kan eksempelvis omfatte en enkeltbehandling av personopplysninger, eller den kan omfatte et helt system. Vurderingen skal handle om personene kommunen har personopplysninger om («de registrerte). Personvernforordningen definerer når det er nødvendig å gjøre en PVK, hva den skal inneholde og hvem som skal gjennomføre den.[[1]](#footnote-2)

## Når skal en vurdering av personvernkonsekvenser gjennomføres?

Kommunen skal vurdere om PVK er nødvendig ved alle endringer og behandlinger som har personopplysninger. Hvis det ikke er behov for en PVK, bør man dokumentere hvorfor, og innhente uttalelse fra personvernombudet.

Det skal alltid gjennomføres en personvernkonsekvensvurdering for behandlinger angitt i Datatilsynets liste:

<https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/>

Typiske tilfeller der det vil være behov for å vurdere personvernkonsekvenser:

* systematisk overvåking av ansatte eller elever
* innføring av ny automatisert tjeneste til brukere
* endringer i et eksisterende system med helseopplysninger
* behandlinger i stor skala av særlige kategorier personopplysninger
* ved bruk av innovativ teknologi

## Hvordan skal en vurdering av personvernkonsekvenser gjennomføres?

Vurderingen er delt opp i fire trinn:

Dokumentere

Vurderingen er delt opp i fire trinn: Personvernkonsekvensvurderingen er inndelt i fire trinn. Første trinn er å planlegge gjennomføringen, finne deltakere og møtetid mv. Andre trinn er å dokumentere personvernkravene til behandlingen. Trinn tre er å vurdere konsekvensene. Siste trinn er sluttvurdering av ansvarlig ledelse og personvernombud.

# Planlegge og organisere (trinn 1)

Start med å planlegge og organisere arbeidet. Antall deltakere og deres rolle må sees i sammenheng med omfang og kompleksitet på behandlingen. Vurder følgende roller:

* Fra kommunen: leder, produkteier, systemeier, saksbehandler, systemansvarlig, representanter fra arkitekturmiljø eller andre roller fra IT-avdelingen, jurist eller sikkerhetsseksjonen mv.
* Representant(er) for den registrerte kan delta i deler av arbeidet.
* Databehandler(e) som er involvert i behandlingen.
* Personvernombudet bør trekkes inn tidlig i vurderingen for råd og veiledning.

Personvernkonsekvensvurderingen skal ha en definert eier. Eier er ansvarlig for risikoene ved behandlingen og skal godkjenne vurderingen. Dette vil følge linjeansvaret i kommunen. Det er også eiers ansvar å beslutte om man skal gå videre med endringen eller utviklingen, skrinlegge planene, eller om det er behov for å eskalere godkjenningen til et høyere nivå i linjen. En PVK er ikke ferdigstilt før eier har godkjent/ikke godkjent vurderingen.

## Behandlingsansvarlig

|  |  |
| --- | --- |
| Hvem er behandlingsansvarlig?  |  |
| Er det flere enn kommunen som er behandlingsansvarlig? (delt eller felles behandlingsansvar)  |  |

## Registrertes representanter

|  |  |
| --- | --- |
| Skal representant for den registrerte involveres?  |  |

## Hvordan involvere personvernombudet

Personvernombudet skal *på anmodning* gi *råd og kontrollere* gjennomføringen av konsekvensvurderingene. Ombudet kan ha en viktig rolle med å bistå den behandlingsansvarlige i vurderingen. Ombudet skal ikke godkjenne konsekvensvurderingene.

|  |  |
| --- | --- |
| Hvordan ble personvernombudet involvert i arbeidet med denne personvernkonsekvensvurderingen?  |  |

## Bakgrunn

|  |  |
| --- | --- |
| Er denne personvernkonsekvens-vurderingen basert på en tidligere gjennomførte PVK eller fra en annen virksomhet?  |   |

## Deltakelse i vurderingen

|  |  |
| --- | --- |
| Navn | Rolle |
|  |   |
|  |   |
|  |   |
|  |   |
|  |  |
|  |  |

## Endringslogg

|  |
| --- |
| Endringslogg |
| Dato | Endringer: | Signert av eier av PVK: |
|  |  |  |
|   |  |  |
|   |  |  |
|   |  |  |

# Dokumentasjon av behandlingen (trinn 2)

Første del av vurdering av personvernkonsekvenser er å beskrive behandlingen av personopplysningene og om personvernprinsippene vil bli ivaretatt. Dette vil tilsvare deler av behandlingsoversikten. Finnes det en behandlingsoversikt kan denne legges ved som utklipp i vedlegg 3.

## Matrise

|  |  |  |
| --- | --- | --- |
|  | Tema  | Dokumentasjon av behandlingen |
| Oversikt over personopplysninger | Hvem er daglig ansvarlig?  |  |
| Hva er formålet med behandlingen?  |  |
| Beskriv hvorfor og hvordan behandlingen skjer |  |
| Er formålet klart nok? Gir det tilstrekkelig veiledning til å kunne vurdere hvilke opplysninger som er relevante for formålet?  |  |
| Finnes det mindre personverninngripende alternativer for å oppnå det samme formålet? (f.eks. anonymisering eller pseudonymisering) |   |
| Hvilke kategorier personer (registrerte) behandles? |  |
| Hvilke typer personopplysninger behandles?Beskriv også omfanget (hvor mange i antall eller prosent) |  |
| Behandles sensitive personopplysninger (særlige kategorier)? |   |
| Behandlingsgrunnlag | Hva er grunnlaget for behandlingen? Begrunn.Ved bruk av 6(1)(a) eller 6(1)(f) må vedlegg 1 eller 2 fylles ut |  |
| Oppleves behandlingen som rimelig? Hva er forventede fordeler ved behandlingen, for kommunen, den registrerte, samfunnet etc. |  |
| De registrertes rettigheter | Hvordan ivaretas åpenhet i behandlingen? Beskriv behov for tiltak som personvernerklæring, informasjonsskriv og annet som gjør at den registrerte vet og forstår hva som skjer. |  |
|  | Hvordan er den registrertes rett til innsyn ivaretatt? |  |
|  | Hvordan håndteres retting og sletting etter krav fra den registrerte? |  |
|  | Kan den registrerte protestere mot automatiserte avgjørelser? |  |
| Innsamling, lagring og sletting | Hvor er opplysningene samlet inn fra? |  |
| Kan formålet oppnås ved å begrense innsamlingen, bruke mindre detaljerte personopplysninger eller å unngå å bruke fortrolige/sensitive opplysninger? |  |
| Hvilke IKT-systemer brukes i behandlingen? |  |
| Hva er planlagt slettefrist? Er det laget sletterutiner? |  |
| Har systemet gode muligheter for å slette automatisk etter tidsfrister eller andre kriterier?  |  |
| Skal personopplysninger anonymiseres fremfor slettes? Nærmere beskrivelse. |  |
| Vurder hvilke garantier som må være på plass dersom personopplysninger skal lagres i lengre perioder grunnet arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål.  |  |
| Utlevering og overføring | Ved bruk av databehandlere (ekstern leverandør), angi hvem dette er |  |
| Er det inngått databehandleravtale med ekstern leverandør? |  |
| Utleveres opplysningene til land utenfor EU/EØS, ev hvilke land? |  |
| Utleveres opplysningene til myndigheter eller andre? |  |
| Riktighet | Beskriv hvordan opplysningene holdes korrekte og oppdaterte, med og uten den registrertes involvering |  |
| Beskriv funksjonalitet for å rette og slette uriktige opplysninger |  |
| Sikkerhet | Hvilke tekniske og organisatoriske tiltak er gjennomført? (Kan overføres fra behandlingsoversikten) |  |

## Risikovurdering av informasjonssikkerheten

Det skal gjennomføres en risikovurdering av *informasjonssikkerheten* før oppstart av nye behandlinger og ved endringer i eksisterende behandling. Risikovurderingen skal identifisere områder som kan gi risikoer knyttet til tilgjengelighet, konfidensialitet og integritet for kommunen. Målet er å identifisere og gjennomføre behov for tiltak for å oppnå et akseptabelt sikkerhetsnivå.

Dersom vurdering av personvernkonsekvenser gjøres for flere systemer, så må risikovurderinger foreligge for alle systemer som er omfattet.

Kommunens maler og veiledning for risikovurdering finner du i [sett inn]

|  |
| --- |
| Dokumentasjon av risikovurderingen |
| Hvor er dokumentasjon knyttet til risikovurderingen lagret? | [Henvisning eller lenke til lagret dokument] |
| Hva dekker risikovurderingen? |  |
| Er det gjenstående risikoer som ikke har tilstrekkelige tiltak? Hvis «JA», gi en beskrivelse av risikoen(e):  |  |

# Vurdering av personvernkonsekvenser for den enkelte (trinn 3)

Personvernkonsekvenser for de registrertes rettigheter og friheter skal vurderes. Det er viktig å ta perspektivet til de(n) registrerte og vurdere hvordan behandlingen vil påvirke personvernet til den enkelte.

Konsekvensen av at rettigheter og friheter ikke blir innfridd kan være både fysisk, materiell og ikke-materiell skade. Konsekvensene for de registrerte er ikke avhengig av at det skjer en uønsket hendelse. Det kan like fullt være at behandlingen i seg selv forhindrer eller begrenser den enkeltes mulighet til å utøve sine rettigheter. Tilpass scenarioene slik at de samsvarer med det aktuelle prosjektet. Fjern scenarioer som ikke er aktuelle. Tabellen under viser noen eksempler.

En beskrivelse av konsekvensnivåene finnes i vedlegg 1. Vedlegg 2 beskriver flere eksempler på risikoer.

## Vurdering av personvernkonsekvenser

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nr | Risiko | Beskrivelse av nåsituasjonen | Konse-kvens (1-5) | Begrunnelse for konsekvens for den enkelte | Forslag til nye tiltak |
| 1 | Liten åpenhet om behandling. Den registrerte får ikke informasjon om behandlingen. |  |  |  |  |
| 2 | Den registrerte får ikke innsyn i egne opplysninger. |  |  |  |  |
| 3 | Behandlingen er diskriminerende som følge av forskjellsbehandling. |  |  |  |  |
| 4 | Behandlingen går ut over det rettslige grunnlaget og skiller ikke mellom hvilke opplysninger som er nødvendig å behandle, og hvilke opplysninger det kan være valgfritt å oppgi. |  |  |  |  |
| 5 | Formålet er ikke tilstrekkelig avklart ved oppstart av behandlingen. |  |  |  |  |
| 6 | Personopplysninger brukes til et annet formål enn det opprinnelige. |  |  |  |  |
| 7 | Det samles inn flere opplysninger enn det som er nødvendig for formålet. Formålet kan oppnås på mindre inngripende måte.  |  |  |  |  |
| 8 | Opplysningene som behandles er feil, mangelfulle og/eller blir ikke oppdatert.  |  |  |  |  |
| 9 | Den registrerte kan ikke få korrigert eller slettet personopplysninger ved forespørsel. |  |  |  |   |
| 10 | Opplysninger lagres lengre enn det som er nødvendig. Det er ikke satt lagringstid / opplysningene lagres utover fastsatt lagringstid. |  |  |  |   |
| 11 | Det oppbevares flere kopier av informasjon (f.eks. mellomlagring) som ikke er omfattet av slettereglene.  |  |  |  |  |
| 12 | Behandlingen er ikke tilstrekkelig fastsatt eller dokumentert. F.eks. Mangler risikovurderinger eller rutiner. |  |  |  |  |
| 13 | Uklare roller- og ansvarsforhold på området / roller- og ansvar er ikke definert. Ikke definert i hele verdikjeden. |  |  |  |  |

## Tiltak for å redusere risiko

Når risiko og konsekvens for den registrerte er vurdert gjenstår det å iverksette risikoreduserende tiltak. Målet er å oppnå et akseptabelt nivå for å ivareta den registrertes personvern i behandlingen.

Dokumenter de nødvendige tiltakene fra vurderingen over, med referanse til hvilke scenarioer tiltaket skal dekke. Dokumenterer også om det er risiko for personvernet som det ikke er mulig å redusere med de identifiserte tiltakene (restrisiko). Det kan eksempelvis være at sletting av opplysninger må gjøres manuelt, noe som øker risiko for menneskelige feil.

I mange tilfeller er det ikke mulig å ende opp uten risiko. Vurder hvilken risiko vi sitter igjen med etter gjennomførte tiltak, og om ansvarlig eier av vurderingen aksepterer denne risikoen.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Behov for tiltak | Ref. til nr. | Ansvarlig | Frist | Restrisiko? |
| [Oppdatere søknadsskjema med informasjon om hvordan personopplysninger behandles] |  |  |  |  |
| [Gå gjennom seksjonens/avdelingens personopplysninger og sette lagringstid/slettefrister] |  |  |  |  |

## Vurderinger

|  |  |  |
| --- | --- | --- |
| I hvilken grad og på hvilken måte kan behandlingen eller tiltaket gripe inn i retten til privatliv og personvern?  |  |  |
| Er behandlingen av personopplysningene er nødvendige?  |   |  |
| Står konsekvensene for de registrerte i et rimelig forhold til formål og behov?  |    |  |
| Er det anbefalt at behandlingen gjennomføres?  |   |  |

# Avslutning og endelig vurdering (trinn 4)

I siste steg av vurderingen skal:

* personvernombudet gi uttalelse og anbefalinger om vurderingen
* eier av PVK vurderer om man ønsker å følge anbefalingene fra PVO, og dokumentere vurderingene og endringene
* behov for eventuell forhåndsdrøfting med Datatilsynet
* vurderingen godkjennes av ansvarlig eier

## Behandlingsansvarliges vurdering

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

## De registrertes (representant) sin vurdering

|  |  |
| --- | --- |
| Hvordan er den registrertes synspunkt hentet inn og ivaretatt i vurderingen?  |   |

## Vurdering og råd fra personvernombudet

Når personvernkonsekvensvurderingen er gjennomført skal den oversendes personvernombudet for uttalelse. Personvernombudets uttalelse skal ikke fjernes, selv om det gjøres endringer i PVK i etterkant. Slik vil det være klart hvilke anbefalinger som er fulgt og/eller dokumentert.

|  |  |  |
| --- | --- | --- |
| Spørsmål for personvernombudet | (ja/nei/usikker)  | Kommentarer |
| Er behandlingen tilstrekkelig beskrevet? (Tydelig, forståelig, deltakelse) |  |  |
| Er vurdering av prinsippene gjennomført? |  |  |
| Er personvernkonsekvenser for den enkelte tilstrekkelig vurdert?  |  |  |
| Vurderes tiltakene tilstrekkelige for å ivareta personvernet? (Ansvarsfordeling, realistiske frister, samsvar mellom konsekvenser og tiltak, restrisiko beskrevet tilstrekkelig?) |  |  |
| Anbefaling fra personvernombudet?  |
| [Anbefaler å gå videre med behandlingen som planlagt][Anbefaler å gå videre med behandlingen og at X, Y, Z endres/gjennomføres/vurderes][Anbefaler å gå videre forutsatt at X, Y, Z endres/gjennomføres][Anbefaler at behandlingen stoppes/ikke iverksettes] |

## Endringer etter vurderingen av personvernombudet

Eier skal dokumentere gjennomførte endringer etter vurdering fra personvernombudet.

|  |
| --- |
| Følgende endringer er gjennomført |
|  |

## Behov for forhåndsdrøftelse med Datatilsynet

Hvis restrisikoen fremdeles er høy og kommunen ikke kan finne tilstrekkelige tiltak for å begrense risikoen, må det foretas en forhåndsdrøftelse med Datatilsynet før behandlingen kan begynne. Personvernombudet koordinerer kontakt med Datatilsynet.

|  |  |
| --- | --- |
| Høy restrisiko |  |
| Er det behov for forhåndskonsultasjon med Datatilsynet? |  |
| Råd eller pålegg fra Datatilsynet:  | [Her skal det refereres til råd eller pålegg fra Datatilsynet eller vises til relevant dokumentasjon som oppsummerer dialogen med Datatilsynet.] |

## Endelig godkjenning

Vurdering skal godkjennes av ansvarlig eier. Når vurderingen er godkjent, skal det ikke gjenstå høy restrisiko. Personvernombudet sine anbefalinger skal også være dokumentert. Dersom eieren av PVK velger å ikke følge anbefalingene fra personvernombudet, skal dette valget begrunnes. Hvis risikoen påvirker andre ansvarsområder, må den godkjennes av rådmannen.

|  |  |
| --- | --- |
| Spørsmål for eieren av PVK | Besvarelse |
| Er anbefalinger fra personvern-ombudet fulgt? Hvis ikke, hva er begrunnelsen for at personvernombudets anbefalinger ikke følges?  |  |
| Godkjenning av «Vurdering av personvernkonsekvenser»  |
| Dato: |  Ansvarlig risikoeier  |

# Vedlegg

## Konsekvenskategorier og konsekvensområder

Konsekvenser beskriver skadevirkninger, som en «mulige følger av en hendelse». Konsekvensene vurderes fra lav til høy i en femdelt skala. En hendelse kan ramme ett eller flere konsekvensområder. Det er det mest alvorlige konsekvensområdet som bestemmer hvor høy risikoen er. Beskrivelsene av konsekvensene er ikke uttømmende, men en hjelp til å kategorisere og sammenligne mellom ulike hendelser.

| **Konsekvens (for den registrerte)** | **Økonomi** | **Omdømme** | **Rett til privatliv og friheter\*** | **Helse\*\*** |
| --- | --- | --- | --- | --- |
| **1. Lav** | Ingen/lite økonomisk tap (dagslønn) | Lite eller midlertidig tap av omdømme (nære eller få relasjoner) | Lite eller midlertidig tap av privatliv | Ingen skade eller sykdom |
| **2. Lav til middels** | Forbigående økonomisk tap (ukelønn) | Midlertidig eller begrenset tap av omdømme | Midlertidig tap av privatliv  | Liten og midlertidig skade |
| **3. Middels** | Økonomisk tap av noe varighet (månedslønn) | Midlertidig eller noe tap av omdømme | Varig tap/mindre krenkelse av privatliv | Middels og midlertidig skade |
| **4. Middels til høy** | Betydelig økonomisk tap (flere månedslønner) | Varig eller alvorlig tap av omdømme (medieoppslag eller ryktespredning) | Krenkelse av privatliv (lekkasje av intim/sårbar informasjon) | Større skade og midlertidig sykehusopphold |
| **5. Høy** | Varig og betydelig økonomisk tap (årslønn) | Varig og alvorlig tap av omdømme (større negative medieoppslag) | Høy krenkelse av privatliv (lekkasje av svært intim/sårbar informasjon) | Varig større skade eller varig funksjonsnedsettelse  |

\*) Må sees i sammenheng med grunnlovens bestemmelser i paragraf 102 (Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet)

Konsekvensene skal vurdere de registrertes rett til: **privatliv, kommunikasjonsvern, ytringsfrihet, tankefrihet, bevegelsesfrihet, forbud mot diskriminering, retten til frihet, samvittighets- og religionsfrihet**

\*\*) Forsikringsselskapenes vurderinger på personskade kan brukes

## Eksempler på scenarioer

* Behandlingen kan gi økonomisk tap for den registrerte
* Behandlingen kan ha konsekvens for omdømme til den registrerte
* Behandlingen kan medføre mulighet for stigmatisering
* Behandlingen kan være diskriminerende
* Behandlingen kan medføre forskjellsbehandling blant søkere hos kommunen
* På grunn av mangel på sikkerhet kan behandlingen føre til identitetstyveri eller bedrageri
* Behandlingen kan være en direkte krenkelse av privatlivets fred
	+ Kontrolltiltak på arbeidsplassen som krenker muligheten til privatliv (f. eks videoovervåkning, detaljert tidsregistrering, adgangskontroll)
* Behandlingen kan medføre inngrep i ytringsfriheten eller tankefriheten hos den registrerte
* Behandlingen kan begrense handlefriheten til den registrerte
* Behandlingen kan svekke selvtilliten til den registrerte
* Behandlingen kan medføre at den enkelte ikke får oppfylt sine personvernrettigheter:
	+ Rett til innsyn
	+ Rett til informasjon
	+ Rett til å protestere mot automatisk behandling
	+ Rett til innsigelse
	+ Rett til korrigering
	+ Rett til å bli glemt (sletting)
	+ Rett til dataportabilitet
	+ Rett til begrenset behandling
1. Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger […] (Personvernforordningen), artikkel 35 [↑](#footnote-ref-2)