Direktoratet for e-helse

# Veileder for utfylling av mal for personvernkonsekvensvurdering (DPIA)

HITR 1243:2022

**Publikasjonens tittel:**
Veileder for utfylling av mal for personvernkonsekvensvurdering (DPIA)

**Rapportnummer**
HITR 1243:2022

**Utgitt:**
Februar 2022

**Utgitt av:**
Direktoratet for e-helse

**Kontakt:**
postmottak@ehelse.no

Publikasjonen kan lastes ned på:
**www.ehelse.no**

# Om malen og veiledning til utfylling

Formålet med veilederen er å gi virksomheter i helse- og omsorgssektoren bistand til gjennomføring og dokumentering av personvernkonsekvensvurdering i henhold til kravene i personvernforordningen artikkel 35. Den består av en mal og en veiledning til utfylling av malen. Denne veilederen er en videreutvikling av Direktoratet for e-helses «Mal for DPIA» som ble publisert i 2019.

Veilederen skal bidra til å gjøre prosessen knyttet til personvernkonsekvensvurdering lettere for både erfarne og mindre erfarne dataansvarlige i helse- og omsorgssektoren. Dette skal igjen bidra til å opprettholde godt personvern i sektoren.

Dataansvarlige i helse- og omsorgssektoren behandler et stort omfang av sensitive personopplysninger og personopplysninger om svært personlige forhold. Behandlingen av personopplysninger kan ofte påvirke den registrerte i stor grad, og ha betydning for pasientsikkerheten og hvilken oppfølging den registrerte får. Det er også mange forskningsprosjekter i sektoren som samler inn et stort omfang av personopplysninger. Forskningsprosjektene kan eksempelvis innebære forsøk på å identifisere eller forutse egenskaper hos de registrerte. Dette tilsier at dataansvarlige i helse og omsorgssektoren ofte vil stå overfor behandling av personopplysninger som kan medføre høy risiko for de registrertes rettigheter og friheter og derved ha plikt til å utføre personvernkonsekvensvurdering. For å gi dataansvarlige i sektoren verktøy og støtte som underbygger denne prosessen, har Direktoratet for e-helse videreutviklet den tidligere Mal for DPIA.

Helse- og omsorgssektoren består av virksomheter av svært forskjellig størrelse og karakter. Dataansvarlige som er små virksomheter, kan ha begrenset tilgang til personell med fagkompetanse innen personvernregelverket. Disse virksomhetene kan derfor ha et særskilt behov for detaljerte maler og utfyllende veiledning. Også hos større virksomheter med høy kompetanse innen personvern, kan det være usikkerhet rundt personvernkonsekvensvurderingers innhold og når de skal gjennomføres. Direktoratet for e-helse mener at dette både kan føre til for mange og omfattende personvernkonsekvensvurderinger, og for få og mangelfulle. Dette indikerer at dataansvarlige i sektoren har et særskilt behov for gode verktøy og støtte som underbygger denne prosessen.

Ved å utgi en mal ønsker Direktoratet for e-helse også å legge til rette for gjenbruk og deling av personvernkonsekvensvurderinger både internt i virksomheter og mellom virksomheter. Det vil være mulig å gjøre tilpasninger i malen, men det anbefales ikke å gjøre dette i større grad enn nødvendig. Det vil være enklere å gjenbruke og dele personvernkonsekvensvurderinger dersom sektoren bruker en lik standard mal.. Dersom virksomhetene velger å ikke benytte seg av noen felter kan disse stå åpne i stedet for å endre i malen.

Denne veilederen består av to deler; en mal og en veiledning til utfylling av malen. Malen for personvernkonsekvensvurdering kan brukes på flere måter og kan tilpasses virksomhetens behov. Veiledningen inneholder veiledning om hva en personvernkonsekvensvurdering er, hvordan malen kan brukes, veiledning til hvert enkelt punkt i malen og en oversikt over viktige begreper som brukes i malen. Se mer om dette i kapittelet «Om mal og veileder».

**Om personvernkonsekvensvurderinger**

En personvernkonsekvensvurdering (Data Protection Impact Assessment, DPIA) skal sikre at personvernet til dem som er registrert i løsningen ivaretas. Dette er en plikt etter Personvernforordningen (GDPR) artikkel 35. Dataansvarlig skal alltid vurdere hvilken risiko en behandling av personopplysninger gir for de registrertes rettigheter og friheter.[1] Hvis det er sannsynlig at en behandling medfører høy risiko for de registrerte, så skal den også utføre en personvernkonsekvensvurdering.

Det anbefales å starte arbeidet med å kartlegge sentrale personvernspørsmål og vurdere ivaretakelse av rettigheter og friheter så tidlig som mulig og allerede før det foreligger et løsningskonsept. En slik tidlig overordnet vurdering av personvernspørsmål vil kunne fungere som underlag for å gjennomføre en personvernkonsekvensvurdering etter artikkel 35.

Personvernkonsekvensvurdering er en prosess som skal beskrive behandlingen av personopplysninger, og vurdere om den er nødvendig og proporsjonal. Den skal også bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og beslutte risikoreduserende tiltak[2].

Personvernkonsekvensvurderinger skal minst inneholde:

- en systematisk beskrivelse av behandlingsaktivitetene av helse- og personopplysninger
- beskrivelse av formålet med behandlingen
- en vurdering av om behandlingene av helse- og personopplysninger er nødvendige og står i rimelig forhold til formålet
- en vurdering av risikoen for personvernet til den registrerte
- planlagte risikoreduserende tiltak for ivaretakelse av personvernet

Personvernkonsekvensvurdering skal ta utgangspunkt i den registrertes perspektiv. Slik skiller personvernkonsekvensvurderinger seg fra andre risikovurderinger, som typisk tar utgangspunkt i perspektivet til virksomheten.

Dokumentasjonen som gjøres i en personvernkonsekvensvurdering vil være viktig for å synliggjøre etterlevelse av virksomhetens arbeid med personvern, og er en viktig brikke i virksomhetens internkontroll og risikostyring.

Alle som behandler personopplysninger, skal vurdere konsekvenser av behandlingen for den registrerte. Virksomheten skal dokumentere lovligheten av behandlingen (behandlingsgrunnlag), formålet, hvordan personvernet til den registrerte er ivaretatt, og at det er gjort tilstrekkelige tiltak for å håndtere risikoen. Dette er krav som Personvernforordningen stiller for alle behandlinger av personopplysninger. Hvordan disse ivaretas bør være en sentral del av virksomhetens internkontroll.

Flere virksomheter i helse- og omsorgssektoren synes det er vanskelig å sikre lovlig grunnlag (behandlingsgrunnlag) for å behandle personopplysninger. Dette er en av de oppgavene som virksomheten skal gjøre for alle behandlinger av personopplysninger. Virksomheten bør ha identifisert et riktig behandlingsgrunnlag før det er aktuelt å gjøre en

[1] Se personvernforordningen artikkel 24 nr. 1

[2] Se Datatilsynets nettsider om DPIA, plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/

personvernkonsekvensvurdering. Mer om behandlingsgrunnlag hos Datatilsynet[3] og i Normens faktaark Formål og behandlingsgrunnlag[4].

Virksomhetene i helse- og omsorgssektoren har ulike kompetanse og kapasitet til dette arbeidet. Noen har gode rutiner og internkontrollsystemer for å ivareta dette, andre har behov for mer veiledning og bistand.

Hvis virksomheten støter på utfordringer underveis i en personvernkonsekvensvurdering, så bør den vurdere å fullføre vurderingen likevel. Utfordringen kan for eksempel være usikkerhet om virksomheten klarer å ivareta enkelte plikter etter personvernforordningen, eller usikkerhet knyttet til om virksomheten vil klare å redusere en risiko til akseptabelt nivå. En ferdigstilt vurdering vil kunne belyse både fordeler og ulemper for de registrerte, og gi ledelsen et godt grunnlag for å ta sin beslutning. En ferdigstilt vurdering vil også være nødvendig dersom virksomheten skal gjennomføre en forhåndsdrøfting med Datatilsynet, eller hvis virksomheten skal oppdatere vurderingen når ny teknologi, nye rettslige avklaringer eller ny informasjon blir tilgjengelig.

Det er ofte aktuelt å gjennomføre personvernkonsekvensvurderinger i forbindelse med anskaffelsesprosesser. Ved anskaffelser bør virksomheten starte med personvernkonsekvensvurderingen så tidlig som mulig, og gjerne sammen med at virksomhetens behov blir spesifisert. På denne måten kan prosessen med personvernkonsekvensvurderingen blant annet hjelpe virksomheten med å utforme krav i konkurransegrunnlaget. Det vil imidlertid være behov for å revidere personvernkonsekvensvurderingen underveis i den videre prosessen med anskaffelsen når virksomheten vet mer om hvordan den endelige løsningen vil se ut.

### Målgruppe

Alle virksomheter og ansatte som skal gjennomføre og bidra i en personvernkonsekvensvurdering kan ha nytte av dette dokumentet.

Malen er tilpasset helse- og omsorgssektoren generelt og retter seg ikke mot spesifikke deler av sektoren.

Formålet er at malen skal være anvendelig, uavhengig av kompetansenivå. Det vil være varierende behov for veiledning blant virksomhetene i sektoren, både med hensyn til utfyllingen av selve malen og til gjennomføring av en personvernkonsekvensvurdering. Både malen og veiledning til utfylling av malen har henvisninger til mer veiledningsmateriell. Noen virksomheter vil trenge ytterligere veiledning til gjennomføringen av selve personvernkonsekvensvurderingen enn det som finnes i denne veilederen.

### Bruk av malen

Denne veilederen består av to deler; en mal og en veiledning til utfylling av malen. Begge dokumenter finner du på ehelse.no

[3] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/
[4] https://www.ehelse.no/normen/faktaark/faktaark-56--formal-og-behandlingsgrunnlag

Det er begrenset med forklaringstekster, veiledningstekster og eksempler i malen. Veilederen til utfylling inneholder forklaringer, eksempler, sjekklister og kontrollspørsmål. Bruk av veilederen til utfylling vil bidra til at feltene i malen forstås og brukes på riktig måte.

Malen deles inn i fem deler;

- DEL A inneholder kjerneinformasjon som beskriver ansvar og roller samt organiseringen av vurderingsprosessen.
- DEL B dekker selve behovsvurderingen av om virksomheten har en plikt til å utføre en personkonsekvensvurdering.
- DEL C omfatter en beskrivelse av behandlingen av personopplysninger, inkludert behandlingens lovlighet (rettsgrunnlag).
- DEL D omfatter selve vurderingen av personvernkonsekvensene.
- DEL E omfatter innspill fra de registrerte og personvernombudet og dokumentasjon på virksomhetens beslutning.

Malen for personvernkonsekvensvurdering kan brukes på flere måter og kan tilpasses virksomhetens behov. Del A (Kjerneinformasjon) fylles ut uavhengig av hvilken måte virksomheten bruker malen på. Det er mulig å bruke malen for å få oversikt over konsekvenser for alle behandlinger av personopplysninger. Virksomheten kan bruke del A, B og C for alle behandlinger, og del D og E for å gjøre personvernkonsekvensvurdering etter personvernforordningens artikkel 35, når det er påkrevet fordi det er sannsynlig at en behandling medfører høy risiko for de registrerte.

**Eksempel 1 Virksomheten har allerede beskrevet og gjort en innledende vurdering av behandlingen av personopplysninger og ført aktivitetene i egen protokoll.**

I dette tilfelle vil det være hensiktsmessig å starte med del B først. Dersom virksomheten konkluderer med at den må gjennomføre en fullstendig personvernkonsekvensvurdering i del B, fortsetter den til del C, D og E.

**Eksempel 2 Virksomheten mangler tilstrekkelig oversikt over den planlagte behandlingen av personopplysninger**

I dette tilfelle kan det være lurt å starte med del C først. Når virksomheten har skaffet seg god nok oversikt over behandlingen av personopplysninger, så kan den fortsette med vurderingen i del B.

Det vil ikke alltid være nødvendig å fullføre del C før virksomheten kan gå tilbake til vurderingen i del B. Et eksempel på dette kan være der virksomheten bruker del C for å skaffe nok informasjon om behandlingen for å kunne vurdere om det skal gjennomføres en personvernkonsekvensvurdering. Det vil i de fleste tilfeller ikke være nødvendig å fylle ut samtlige felter for å kunne gjøre denne vurderingen.

Virksomheten må vurdere om det er nødvendig å fylle ut dataflyt, bruk av leverandører eller *hvordan* registrertes rettigheter skal oppfylles, for å ta kunne ta stilling til om behandlingen faller inn under Datatilsynets liste eller kravene til Artikkel 29-gruppen.

Det kan være lurt å ta utgangspunkt i kriteriene fra Artikkel 29-gruppen del B skal brukes til dette formålet. På denne måten har virksomheten en standard å forholde seg til med tanke på informasjonen den trenger å fylle ut for å deretter gjøre personvernkonsekvensvurderingen.

## Begreper som brukes i malen og veiledningen

Nedenfor er noen viktige begrep i malen forklart. For flere forklaringer og begreper, se personvernforordningen og definisjoner i Normen[5].

**Behandling**
Begrepet «behandling» betyr her enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, 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.

**Behandlingsaktivitet**
Behandlingsaktiviteter er en oversikt over alle aktiviteter hvor personopplysninger behandles i virksomheten. Dersom det er hensiktsmessig, kan virksomheten velge å kategorisere eller gruppere typer aktivitet. I beskrivelsen av en aktivitet, kan det for eksempel være nyttig å opplyse om hvorvidt aktiviteten er knyttet til innsamling, intern bruk eller tilgjengeliggjøring/utlevering.

Et eksempel på en behandlingsaktivitet er der en virksomhet fører en oversikt over ansatte i et HR-system. I selve systemet registreres det personopplysninger som navn, adresse, telefonnummer, navn på nærmeste pårørende etc. Formålet med systemet er å behandle personopplysninger om ansatte for å kunne utbetale lønn, registrere sykefravær og annen relevant informasjon.

**DPIA-veileder utarbeidet av Artikkel 29-gruppen:**
Artikkel 29-gruppen var tidligere den øverste rådgivende forsamlingen for EU-kommisjonen i spørsmål om personvern og informasjons-sikkerhet. De utarbeidet bl.a. veiledere som sa noe om hvordan personvernregelverket skulle forstås, blant annet veileder for personvernkonsekvensvurdering (DPIA)[6]. De er derfor en viktig kilde til hvordan personvernregelverket skal fortolkes. Etter GPDR er Artikkel 29-gruppen erstattet av Det europeiske personvernrådet (EDPB).

Datatilsynets veiledere vil bygge på veiledere fra Art. 29-gruppen. På Datatilsynets nettsider vil man finne den norske oversettelsen[7].

**Dataansvarlig:**
Dataansvarlig er den som er «ansvarlig for behandling av helseopplysninger etter personvernforordningen artikkel 4 nr. 7.» jf. pasientjournalloven § 2.

---

[5] https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren#6%20Vedlegg
[6] https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en
[7] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-er-risiko-hoy/ og https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/edpbartikkel29gruppen/Veileder-i-vurdering-av-personvernkonsekvenser-wp-248-norsk.pdf

Begrepet dataansvarlig brukes i helselovgivningen istedenfor behandlingsansvarlig.

Dataansvarlig er «en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den dataansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett» jf. personvernforordningen artikkel 4. nr.7.

**Databehandler**
I personvernforordningen artikkel 4 nr. 8 angis det at en databehandler er en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.

**Formål og behandlingsgrunnlag[8]**
Den dataansvarlige må definere minst ett formål for hver behandling av personopplysninger den utfører. I tillegg må dataansvarlig sikre at behandlingen oppfyller kravene til et av behandlingsgrunnlagene i personvernforordningen artikkel 6 nr. 1. Gjelder behandlingen personopplysninger som er gitt et ekstra vern (f.eks. helseopplysninger, etnisitet eller religion), så er det tilleggskrav i personvernforordningen artikkel 9.

**Høy risiko**
Det finnes ikke en tydelig definisjon i personvernforordningen av hva som betegnes som høy risiko, men man kan finne noe veiledning i fortalens punkt 76.

*«Hvor sannsynlig og alvorlig risikoen for den registrertes rettigheter og friheter er, bør fastslås ut fra behandlingens art, omfang, formål og sammenhengen den utføres i. Risikoen bør vurderes ut fra en objektiv vurdering der det fastslås om behandlingen av personopplysningene innebærer en risiko eller en høy risiko.»*

Datatilsynet[9] har angitt hva som anses å inngå i «art, omfang og sammenheng». Det anbefales derfor å ta utgangspunkt i dette når man vurderer hva som skal anses som høy risiko.

**Personopplysning**
Opplysning eller vurdering som kan knyttes til en enkeltperson. Dette kan bl.a. være navn, adresse, telefonnummer, e-postadresse, bilnummer, bilder eller fødselsnummer.

**Registrert:**
Den som opplysningene kan knyttes til. Eksempler og begreper som brukes om den registrerte kan også være søker, pasient/bruker, ansatte, deltager i forskningsprosjekt, pårørende og tjenestemottaker.

**Rettigheter og friheter**:
De registrertes rettigheter etter personvernforordningen kapittel 3, men også helserettigheter og andre grunnleggende menneskerettigheter som retten til privatliv,

[8] Les mer om Formål og behandlingsgrunnlag her https://www.ehelse.no/normen/faktaark/faktaark-56--formal-og-behandlingsgrunnlag
[9] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-er-risiko-hoy/

kommunikasjonsvern, ytringsfrihet, tankefrihet, bevegelsesfrihet, forbud mot diskriminering, retten til frihet og samvittighets- og religionsfrihet.

**Særlige kategorier av personopplysninger**
Det er visse typer av personopplysninger som er av mer sensitiv art. Tidligere ble de omtalt som sensitive personopplysninger, mens de nå heter særlige kategorier av personopplysninger.

Personvernforordningens artikkel 9 angir at disse opplysningene er forbudt å behandle, men det finnes unntak i artikkel 9 nr. 2 og nr.3.

Det som anses som særlig kategori av personopplysninger er *helseopplysninger, genetiske opplysninger, biometriske opplysninger (når behandlingsformålet er å entydig identifisere noen), opplysninger om seksuelle forhold og seksuell legning, opplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning, fagforeningsmedlemskap,*

Dette er veiledning til utfylling av malen. Malen ligger på ehelse.no

# A. Kjerneinformasjon

Her skal virksomheten dokumentere kjerneinformasjon om ansvarsforhold, roller og organiseringen av vurderingsprosessen. Her vil den få oversikt over behandlinger/prosess som skal vurderes, hvilke roller og/eller fagkompetanse som har deltatt i vurderingen, samt versjonshistorikk og eventuelle vedlegg.

### A 1. Navn på dataansvarlig virksomhet

Oppgi navn på dataansvarlig virksomhet.

### A 2. Hvilken rolle har virksomheten?

Utgangspunktet i Personvernforordningen er at dataansvarlig har ansvaret for å gjennomføre personvernkonsekvensvurderinger.

Dersom virksomheten har felles dataansvar med en annen virksomhet, skal dette oppgis her. Ved felles dataansvar kan det være variasjoner i oppgavefordelingen. Dette bør beskrives i personvernkonsekvensvurderingene under de punktene der det er relevant. Det kan for eksempel være relevant å beskrive dette under punktet om dataflyt), andre relevante forhold) og ved selve personvernkonsekvensvurderingen, for eksempel dersom selve oppgavefordelingen utgjør en risiko for de registrertes rettigheter og friheter. Den registrerte skal kunne utøve sine rettigheter overfor hver enkelt av de dataansvarlige. Det bør gå frem av dokumentet dersom det er avtalt mellom de dataansvarlige at en av partene har ansvar for gjennomføring av personvernkonsekvensvurderingen. Dette skal følge av en ordning mellom partene, jf. personvernforordningen artikkel 26 nr. 2. Dersom virksomhetene har en avtale som regulerer oppgavefordelingen, bør denne legges til som vedlegg.

Når flere virksomheter skal utføre behandlingsaktiviteter som skal dekkes av samme personvernkonsekvensvurdering, er utgangspunktet at hele behandlingen dekkes av en personvernkonsekvensvurdering, som gjennomføres av virksomheten som har dataansvaret.

Ved behandling av helseopplysninger i for eksempel et forskningsprosjekt på tvers av virksomheter (multisenterstudie) vil rollen som forskningsansvarlig og dataansvarlig normalt være sammenfallende. Dersom de andre virksomhetene som deltar i behandlingen/forskningsprosjektet ønsker å bli involvert i vurderingen, bør dette avklares tidlig i prosessen og meldes til dataansvarlig. Det er ledelsen hos virksomheten som har dataansvaret som skal ta stilling til risikoen ved behandlingen, ikke ledelsen i samtlige virksomheter. Virksomhetene uten dataansvar som har innspill til vurderinger, beskrivelser av faktiske forhold eller risikoen ved behandlingen, bør spille inn disse på et tidlig tidspunkt. På denne måten vil personvernkonsekvensvurderingen i større grad dekke den faktiske risikoen og lede til et bedre beslutningsgrunnlag for ledelsen

Det finnes tilfeller der flere virksomheter deltar i en behandling som det skal gjennomføres en personvernkonsekvensvurdering for. Dette kan være virksomheter (databehandlere) som skal gjennomføre enkelte behandlingsaktiviteter for den dataansvarlige, for eksempel dataanalyse eller lagring. Selv om det er dataansvarlig som har ansvaret for vurderingen kan andre, for eksempel databehandler eller eksterne konsulenter, bidra i utfyllingen. Dette kan

for eksempel være nødvendig ved utfylling av punkt om dataflyt. Virksomheten skal da føres opp i oversikten over deltakere.

### A 3. Navnet på prosjektet/prosessen/systemet/løsningen som skal vurderes

Sett inn navnet på prosjektet/prosessen/systemet/løsningen.

Benytt et navn som gjør vurderingen lett å finne igjen, for eksempel navn på system som skal kjøpes inn.

### A 4. Overordnet beskrivelse av prosjektet/prosessen/systemet/løsningen som vurderes og eventuelle avgrensninger:

Virksomheten kan bruke punktet til å kort, presist og overordnet beskrive prosjektet/prosessen/systemet/løsningen som skal vurderes.

Eventuelle forutsetninger og avgrensninger for vurderingen bør også tas med. Virksomheten kan for eksempel også synliggjøre eventuelle vurderinger den har gjort tidligere, og definere hvilke deler av et system som er gjenstand for vurderingen, hvis den ikke gjelder hele systemet.

### A 5. Databehandlere, leverandører og andre relevante parter

Her skal virksomheten liste opp databehandlere, leverandører og andre parter som er relevante for prosjektet/prosessen/systemet/løsningen som skal vurderes. Dette feltet er kun ment som en oversikt og skal ikke gi utdypende forklaringer på hvordan de ulike aktørene er involvert i prosessen som vurderes eller prosessen med å gjennomføre personvernkonsekvensvurderingen. Dette skal dokumenteres i øvrige punkter i malen, for eksempel i punktet om databehandlere og relasjonen til og mellom disse og punkt om deltakere i vurderingen.

### A 6. Deltakere i vurderingen

Her skal det oppgis hvem som har deltatt i utfyllingen av malen og ellers i personvernkonsekvensvurderingen. Virksomheten dokumenterer her hvilke personer som har deltatt, hvilken rolle de har og ellers annen informasjon om deltakelsen. Det kan være nyttig å synliggjøre hvilke deltakere som har deltatt i deler av prosessen, for eksempel bare i beskrivelsen av behandlingen (del C) eller i vurderingen av personvernkonsekvenser (del D). Dette for å synliggjøre og dokumentere hvilken fagkompetanse som har vært involvert eller rådført. Dersom alle relevante parter har vært involvert og har fått anledning til å uttale seg, vil den samlede vurderingen bli bedre og mer komplett. Det vil også være lettere å revidere vurderingen i fremtiden, da det er lett å identifisere hvilke roller som skal involveres.

I noen tilfeller bidrar databehandlere, leverandører eller andre med utfyllingen. Dette må dokumenteres her. I kommentarboksen bør det da spesifiseres hva de har bidratt med og omfanget av bidraget.

Deltakerne i vurderingen, bør samlet ha bred kompetanse om behandlingen. Deltakerne bør ha kompetanse innen:

- Systemer (f.eks. systemansvarlig)
- Personvern
- Innkjøp
- Utførelse av selve behandlingen av personopplysninger (f.eks. ansatte)
- IT
- Informasjonssikkerhet
- Leverandører/databehandlere

I tillegg bør personvernombudet og representanter for den registrerte delta i personvernkonsekvensvurderingen.

### A 7. Beskriv når og hvordan personvernombudet har blitt involvert

Her skal virksomheten beskrive om og hvordan personvernombudet har vært involvert i prosessen før selve personvernkonsekvensvurderingen gjennomføres. Det finnes ulike måter ombudet kan være inkludert på. Virksomhetens retningslinjer for når og hvordan personvernombudet skal involveres vil variere fra virksomhet til virksomhet. Det kan være en fordel å involvere ombudet tidlig i prosessen. Personvernombudet sitter på viktig kompetanse og vil kunne gi veiledning som gjør prosessen smidigere og raskere.

Hvis virksomheten ikke har personvernombud (PVO), kan dette registreres under dette punktet.

Under følger eksempler på hvordan personvernombudet kan bli involvert i prosessen:

Eksempel 1
Lillevik sykehus skal gjennomføre personvernkonsekvensvurdering av et nytt journalsystem. Før de setter i gang med vurderingen, innkaller de PVO til et møte og informerer om den planlagte behandlingen, og ombudet kommer med spørsmål og innspill. Virksomheten har rutiner for gjennomføring av personvernkonsekvensvurderinger som PVO viser til. Ombudet gir også en kort innføring i de registrertes rettigheter og hva som menes med vurderinger av nødvendighet og proporsjonalitet, da gruppen er litt usikre på dette. Gruppen gjennomfører deretter personvernkonsekvensvurderingen uten at ombudet er involvert. Etter at vurderingen er ferdig, sendes dokumentet til PVO. PVO skriver deretter et notat som legges ved vurderingen. PVO kontrollerer at alle de obligatoriske momentene i en personvernkonsekvensvurdering er med, men stiller spørsmål ved om alle mottakere av personopplysningene er oppført i beskrivelsen. Ombudet har også noen forslag til ytterligere risikoreduserende tiltak. Utover dette slutter ombudet seg til vurdering og konklusjon.

Gruppen som gjennomførte personvernkonsekvensvurderingen kontrollerer at mottakere av opplysningene stemmer og gjør en vurdering av om tiltakene er hensiktsmessige, før de sender dokumentet til ledelsen for beslutning.

Eksempel 2
Storevik Legekontor planlegger å ta i bruk et nytt system for digital kommunikasjon med pasientene sine. Legekontoret har ikke internt personvernombud, men har satt ut ombudsfunksjonen en annen virksomhet, som bistår ved behov og ved ledelsens gjennomgang. Legekontoret har hørt at det skal gjennomføres en personvernkonsekvensvurdering ved innføring av større systemer, men er usikre på

hvordan det skal gjøres. De kontakter personvernombudet, som med sin kompetanse og erfaring fungerer som tilrettelegger.

Ombudet veileder legekontoret gjennom hele prosessen og er til stede, men deltar ikke selv aktivt i å vurdere behandlingen. I stedet bidrar ombudet med fortløpende oppklaringer og opplæring, og stiller spørsmål som setter legekontoret i stand til å gjøre vurderingen selv.

Til slutt skriver ombudet en egen vurdering av behandlingen og slutter seg til konklusjonen før ledelsen gjennomgår dokumentet og signerer.

### A 8. Versjonshistorikk

Her skal virksomheten dokumentere når personvernkonsekvensvurderingen sist ble gjennomgått/oppdatert.

I tillegg til planlagt, periodisk gjennomgang, kan det dukke opp behov for gjennomgang/revurdering/oppdatering av personvernkonsekvensvurderingen ved flere anledninger, for eksempel:

- Ved lovendringer som påvirker behandlingen
- Endring i risikobildet, enten generelt eller hvis virksomheter har hatt et brudd på personopplysningssikkerheten
- Endring i selve behandlingen eller formålet, for eksempel ytterligere behandlingsaktiviteter eller endre en pågående behandlingsaktivitet
- Endring i teknisk løsning
- Der personvernkonsekvensvurderingen er basert på en vurdering som er delt fra en annen virksomhet, som omhandler samme/tilsvarende behandling (gjenbruk av personvernkonsekvensvurdering).

Ved store endringer i behandlingen eller i den tekniske løsningen som benyttes, bør det vurderes om hele personvernkonsekvensvurderingen skal gjøres på nytt. I slike tilfeller kan virksomheten gjenbruke tekst og vurderinger som fra den tidligere personvernkonsekvensvurderingen. Dersom virksomheten velger å gjøre en ny vurdering, bør den tidligere personvernkonsekvensvurderingen føres opp i versjonshistorikken. Virksomheten bør også beskrive endringene fra forrige personvernkonsekvensvurdering i behovsvurderingen (malens del B).

### A 9. Oversikt over samtlige vedlegg

Her skal virksomheten føre opp dokumenter som bør ses i sammenheng med vurderingen av personvernkonsekvenser. Virksomheten skal legge ved beskrivelser av løsningen som blir vurdert. Andre vedlegg kan være f.eks. beskrivelse av behandlingen som kommer fra leverandør, styringsdokumenter, rutinebeskrivelser eller annen relevant dokumentasjon.

Dersom det allerede er gjennomført en vurdering av behovet for personvernkonsekvensvurdering (som det legges opp til i malens del B), eller beskrivelse av

behandlingen (malen del C) og dette er dokumentert et annet sted, skal det også føres opp i listen her.

Vedlegg kan refereres til via lenke, eller via en beskrivelse av hvor dokumentet er lagret. Det bør nevnes hva slags dokument det er, versjonsnummer og når dokumentet sist ble endret. Dette bør gjøres for at virksomheten ikke viser til utdaterte rutiner, systembeskrivelser eller annet når personvernkonsekvensvurderingen skal gjennomgås/oppdateres.

**A 10. Arkivnummer/saksnummer eller andre viktige kjennetegn for virksomheten:**

Her kan virksomheten skrive inn arkivnummer, prosjektnummer, saksnummer eller lignende kjennetegn.

**A 11. Beskriv de forskjellige behandlingsaktivitetene som inngår i vurderingen:**

Her skal virksomheten beskrive de forskjellige behandlingsaktivitetene. Det er lurt å ta for seg hver enkelt aktivitet og fylle ut deretter. Det kan være nyttig å opplyse om hvorvidt aktiviteten er knyttet til innsamling, intern bruk eller tilgjengeliggjøring/utlevering. Utlevering av personopplysninger til tredjeparter skal også beskrives under dataflyt i malens del C.

Virksomheten kan velge å kategorisere eller gruppere typer aktivitet. Flere behandlingsaktiviteter kan slås sammen til en mer overordnet aktivitet, så lenge formålet og behandlingsgrunnlaget er det samme.[10] For eksempel vil aktiviteten «Oversending av prøver til analyse og mottak av prøvesvar» inkludere all håndtering av personopplysninger som skjer når det tas en prøve av pasienten, når prøven og opplysninger sendes til laboratoriet, når prøven analyseres og vurderes, og når resultatet returneres til og håndteres av det behandlende helsepersonellet.

Det er viktig å kunne avgrense og beskrive formål(ene) så tidlig som mulig i planleggingen av en behandling av personopplysninger. Det lovlige grunnlaget (behandlingsgrunnlaget) for behandlingen av personopplysninger følger av hva som er formålet man ønsker å oppnå med behandlingen, og av dette lovlige grunnlaget følger også blant annet hvilke rettigheter de registrerte har etter personvernforordningen og hvilke plikter det innebærer for den dataansvarlige. At formål og behandlingsgrunnlag er avklart og kan beskrives er derfor en forutsetning for å kunne gjennomføre en vurdering av personvernkonsekvensene for de registrerte.

[10] Mer informasjon om definering av formål og behandlingsgrunnlag finnes i Normens Faktaark 57 – Personvernprinsippene og Faktaark 56 Formål og behandlingsgrunnlag

| Veiledning til utfylling | |
|---|---|
| Behandlingsaktivitet: | Se kapittel om begrep. |
| Formål: | Her skal ett eller flere formål med behandlingen oppgis. En behandling kan utføres for flere formål. Det bør vurderes om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålet/formålene. Hvis formålet fraviker det opprinnelige formålet opplysningene ble samlet inn for, så bør det tydeliggjøres på dette punktet. |
| Rettslig behandlingsgrunnlag: | Her må virksomheten oppgi rettslig behandlingsgrunnlag etter artikkel 6, men også etter artikkel 9 der det er aktuelt. Virksomheten bør også redegjøre for supplerende rettsgrunnlag eller berettigede interesser dersom det er aktuelt. |
| Personopplysninger som benyttes: | Hvilke typer personopplysninger? |
| Særlige kategorier av personopplysninger som benyttes: | Fyll ut om det behandles opplysninger som tilhører særlig kategorier av opplysninger, personvernforordningen art 9.<br><br>Helseopplysninger er særlig kategori av opplysninger. |
| Lagringstid:[11] | Fyll ut hvor lenge virksomheten planlegger å oppbevare de forskjellige personopplysningene i tid eller kriterier. Sletting på bakgrunn av en forespørsel fra den registrerte (retten til sletting) skal beskrives i malens del C. |

[11] Mer informasjon om definering av formål og behandlingsgrunnlag finnes i Normens Faktaark 57 – Personvernprinsippene og Faktaark 56 Formål og behandlingsgrunnlag

# B. Behovsvurdering

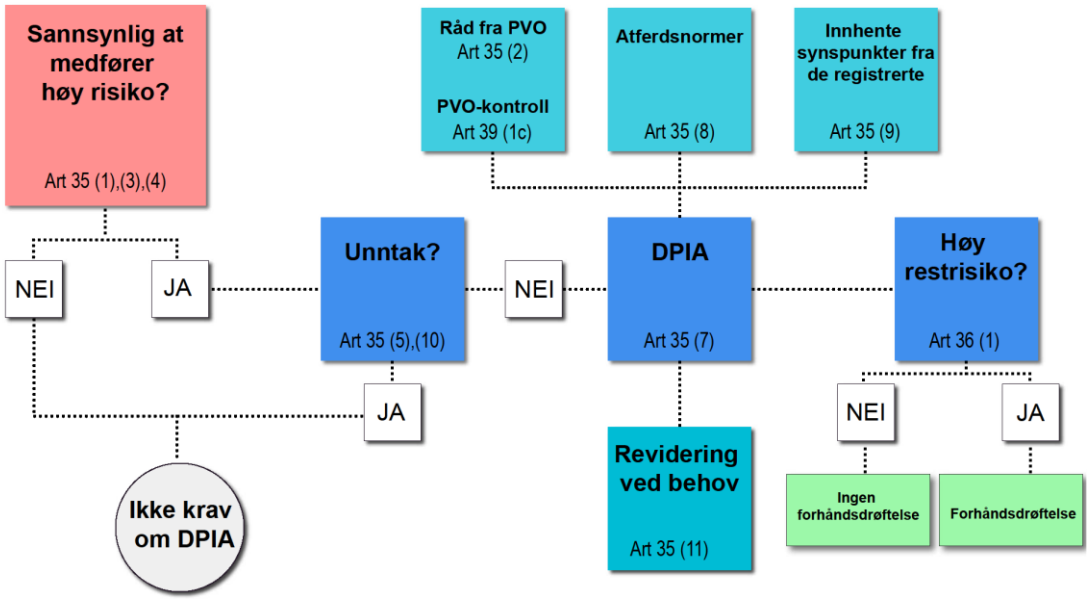
Her skal virksomheten vurdere og dokumentere om det er nødvendig å foreta en personvernkonsekvensvurdering. Kjernen i denne vurderingen er om det er sannsynlig at behandlingen vil medføre høy risiko for de registrertes rettigheter og friheter.

### B 1. Indikasjoner på at personvernkonsekvensvurdering må gjennomføres

Her skal virksomheten identifisere momenter som tyder på at behandlingen vil medføre en høy risiko for de registrertes rettigheter og friheter.

Hva som skal anses som høy risiko er ikke tydelig definert i personvernforordningen. I personvernforordningens fortalepunkt 76 står det at risikoen må fastslås basert på behandlingens art, omfang, formål og sammenhengen den utføres i. Virksomheten må derfor gjøre en konkret vurdering av om behandlingen vil innebære en mer alvorlig inngripen i personvernet enn andre behandlinger basert på disse momentene. Behandlingen kan medføre en høy risiko hvis personopplysningene som behandles er av en særskilt sensitiv karakter, eller hvis måten personopplysningene behandles på utgjør et særskilt inngrep i de registrertes rettigheter og friheter. Datatilsynet har utarbeidet en veileder for hvordan momentene skal vurderes.[12]

Følgende figur illustrerer når vurdering av om behandlingen medfører høy risiko for de registrertes rettigheter og friheter skal gjennomføres. Figuren er basert på figur i DPIA-veileder utarbeidet av Artikkel 29-gruppen.[13]




[12] Les mer om dette her https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-er-risiko-hoy/
[13] https://ec.europa.eu/newsroom/article29/items/611236 og https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/edpbartikkel29gruppen/Veileder-i-vurdering-av-personvernkonsekvenser-wp-248-norsk.pdf

Som illustrasjonen også viser, må virksomheten foreta en vurdering basert på de første punktene før den foretar selve personvernkonsekvensvurderingen. Den kan for eksempel ikke kan gå rett på del C i malen, men må først vurdere innholdet i artikkel 35 (1) og unntak i artikkel 35 (5) og (10).

Virksomheten kan allerede på dette punktet ha identifisert at den aktuelle behandlingen vil føre til høy risiko for de registrertes rettigheter eller friheter og/eller identifisert at behandlingen ikke vil medføre høy risiko for de registrertes rettigheter eller friheter og at det ikke er nødvendig å gjøre en full personvernkonsekvensvurdering. Virksomheten skal dokumentere vurderingen. Dette er viktig særlig hvis forutsetningene for vurderingen endres.

Vurderingen kan endre seg ved innføring av ny teknologi. For eksempel så kan overgang fra manuell saksbehandling til å foreta automatiserte avgjørelser føre til at de registrertes rettigheter og friheter berøres.

**Eksempel**

Lillevik legekontor benytter seg av en app for å lagre personopplysninger (navn, adresse, kjønn) om ansatte. Disse opplysningene blir vurdert som ikke sensitive. Det er dessuten kun den ansatte, den ansattes leder samt noen få underleverandører som vil ha innsyn i disse opplysningene. Noen opplysninger skulle lagres i tredjeland, men dette var i tråd med personvernforordningen på det tidspunktet personvernkonsekvensvurderingen ble gjennomført.

I forkant av nedlastningen av appen ble det gjort en personvernkonsekvensvurdering for å vurdere risikoen for de opplysningene som ble registrert om de ansatte. Risikoen ble ansett som lav.

Et par måneder etterpå kommer det ny rettspraksis som sier at virksomheten ikke kan bruke underleverandører fra land utenfor EU/EØS, noe legekontoret gjorde. Dette medfører til at Lillevik må oppdatere den gjeldende personvernkonsekvensvurderingen, for å kunne ta stilling til om det finnes tiltak som reduserer risikoen ved overføring til tredjeland.

**Behandlingen er oppført i Datatilsynets liste over behandlingsaktiviteter som alltid innebærer høy risiko for de registrertes rettigheter og friheter.**

Det første virksomheten bør gjøre er å vurdere om det finnes behandlinger den vet vil føre til høy risiko.

Datatilsynet har utarbeidet en oversikt over behandlingsaktiviteter som alltid krever at det må gjøres en personvernkonsekvensvurdering. [14]

Virksomheten vurderer om det er et eller flere elementer/alternativer som passer for den behandlingsaktiviteten virksomheten skal gjøre. Etter Datatilsynets vurdering er dette aktiviteter som sannsynligvis alltid vil medføre høy risiko for de registrertes rettigheter og friheter. Det må derfor gjennomføres en full personvernkonsekvensvurdering uavhengig av hvordan virksomheten vurderer risikoen.

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

Selv om behandlingen står på Datatilsynets liste over behandlingsaktiviteter, kan det være nyttig å gjennomgå kravene fra Artikkel 29-gruppens veileder og artikkel 35 i personvernforordningen og se hvilke av kravene som passer på den planlagte aktiviteten. Kravene inneholder gode momenter/risikoer som det kan være hensiktsmessig å ta med seg videre, både når det skal lages en beskrivelse av behandlingen (del C) og når personvernkonsekvensene skal vurderes (del D).

**Et av de alternative kravene i personvernforordningens Artikkel 35 (3) er oppfylt**

Her skal virksomheten vurdere om et av de alternative kravene i art 35(3) er oppfylt.

Personvernforordningens artikkel 35 nr.3 angir noen eksempler på når en behandling «sannsynligvis vil medføre en høy risiko». Vær oppmerksom på at eksemplene ikke er uttømmende.

«En vurdering av personvernkonsekvenser som nevnt i nr. 1 skal særlig være nødvendig i følgende tilfeller:

a) en systematisk og omfattende vurdering av personlige aspekter ved fysiske personer som er basert på automatisert behandling, herunder profilering, og som danner grunnlag for avgjørelser som har rettsvirkning for den fysiske personen eller på lignende måte i betydelig grad påvirker den fysiske personen

b) behandling i stor skala av særlige kategorier av opplysninger som nevnt i artikkel 9 nr. 1, eller av personopplysninger om straffedommer og lovovertredelser som nevnt i artikkel 10 eller

c) en systematisk overvåking i stor skala av et offentlig tilgjengelig område.»

Behandling av særlige kategorier av opplysninger i punkt b) vil omfatte helseopplysninger.

**Kriterier i Artikkel 29-gruppens veileder er oppfylt**

Artikkel 29-gruppen har lagt til grunn ni kriterier som kan benyttes for hjelpe virksomheten med å avgjøre hvorvidt en behandling vil føre til høy risiko eller ikke.[15] Her skal virksomheten vurdere om noen av kriteriene i Artikkel 29-gruppens veileder er oppfylt.

Det er anbefalt å gjennomføre en personvernkonsekvensvurdering dersom to eller flere kriterier er oppfylt, men dette er ikke absolutt. Virksomheten må derfor gjøre en konkret vurdering i tillegg til å velge/krysse av for de relevante kriterier her.

Kriteriene kan benyttes som momenter i vurderingen av om det sannsynligvis foreligger høy risiko for de registrertes rettigheter og friheter. Virksomheten kan komme frem til at det ikke skal gjennomføres en personvernkonsekvensvurdering selv om flere av kriteriene er oppfylt. For eksempel kan en virksomhet behandle store mengder opplysninger om sårbare grupper, men det er lite sensitive data eller pseudonymiserte data[16], som gjør at risikoen anses som lav. Kravet til en god begrunnelse for ikke å gjøre en personvernkonsekvensvurdering blir

[15] https://ec.europa.eu/newsroom/article29/items/611236/en

[16] Les mer om dette her https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/hvordan-anonymisere-personopplysninger/

høyere dess flere kriterier som er oppfylt. Virksomheten kan også komme frem til at det skal gjennomføres en personvernkonsekvensvurdering selv om kun ett av kriteriene er oppfylt.

Datatilsynet har laget en tabell som illustrerer hvordan kriteriene kan anvendes for å vurdere hvorvidt det skal gjennomføres en personvernkonsekvensvurdering.[17]

De ni kriteriene fra Artikkel 29-gruppen er:

- Behandlingen innebærer ***evaluering eller poengsetting av registrerte*.** Dette inkluderer profilering og forutsigelse, spesielt «aspekter som gjelder arbeidsprestasjoner, økonomisk situasjon, helse, personlige preferanser eller interesser, pålitelighet eller atferd, plassering eller bevegelser». [18]
- Behandlingen innebærer ***automatiserte beslutninger*** med rettslig eller tilsvarende betydelig virkning.
- Behandlingen innebærer ***systematisk monitorering***. For eksempel observering, overvåking eller kontroll av de registrerte.
- Behandlingen omfatter ***særlige kategorier av personopplysninger.*** Særlig kategori av personopplysninger er nærmere definert i *artikkel 9* og er for eksempel helseopplysninger eller opplysninger om rase.
- Behandlingen omfatter ***matching eller sammenstilling*** av datasett.
- Behandlingen innebærer behandling av personopplysninger i ***stor skala***. I forordningen angis det ikke hva som menes med stor skala, men relevante faktorer er:
    - Antallet registrerte som berøres, enten som et spesifikt antall eller som en andel av den relevante befolkningen.
    - Mengden og/eller spennvidden i personopplysningene som behandles.
    - Varigheten eller regelmessigheten på databehandlingen.
    - Det geografiske omfanget av behandlingen.
- Behandlingen gjelder ***sårbare registrerte***. Eksempler på sårbare registrerte er barn og pasienter/brukere. Barn er ikke i stand til å motsette seg eller gi samtykke til behandling av personopplysninger, pasienter/brukere anses som sårbare da vedkommende står i et avhengighetsforhold til dataansvarlig/virksomheten.
- Behandlingen innebærer ***innovativ bruk eller anvendelse*** av ny teknologisk eller organisatorisk løsning. Dette betyr bruk av teknologi som er ny for virksomheten som utfører vurderingen av personvernkonsekvenser, ikke teknologi som er generelt ny eller innovativ.
- Behandlingen vil ***hindre de registrerte i å utøve en rettighet*** eller gjøre bruk av en tjeneste eller en avtale.

*Virksomheten har tidligere hatt konsesjon[19] fra Datatilsynet eller godkjenning fra REK som er datert før juli 2018.*

[17] Se tabellen nederst på siden her https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-er-risiko-hoy/
[18] Ref. fortalepunkt 71 og 91.
[19] https://www.datatilsynet.no/regelverk-og-verktoy/konsesjon-og-melding/

Dersom virksomheten tidligere har hatt konsesjon fra Datatilsynet eller godkjenning fra REK bør disse legges til grunn i personkonsekvensvurderingen. På denne måten viser den hva som har blitt godkjent tidligere og hvorfor.

Dersom det er gjort endringer i behandlingen av personopplysninger siden konsesjon eller godkjenning fra REK ble gitt, bør endringene omtales her.

Legg konsesjonen eller godkjenningen til i lista over vedlegg.

**Virksomheten har etter en konkret vurdering kommet til at det sannsynligvis foreligger høy risiko for de registrertes rettigheter og friheter**

Her skal virksomheten dokumentere og beskrive hvilke momenter den har lagt vekt på dersom det er foretatt en konkret vurdering av om det foreligger høy risiko. For å avgjøre om det foreligger høy risiko må virksomheten vurdere behandlingens art, omfang, formål og sammenhengen den utføres i. Datatilsynet har utarbeidet en veileder for hvordan momentene skal vurderes.[20]

Det vil ikke være nødvendig å gjennomføre en slik konkret vurdering dersom behandlingen er listet opp i Datatilsynets liste, men det kan være relevant å gjøre en konkret vurdering selv om virksomheten kan krysse av for andre alternativer. Dette vil særlig være aktuelt dersom noen av kriteriene til Artikkel 29-gruppen er oppfylt. Kriteriene kan benyttes som momenter i denne vurderingen.

### B 2. Har personvernombudet uttalt seg om behovet for å gjennomføre en personvernkonsekvensvurdering?

Før det er besluttet at det skal gjennomføres en personvernkonsekvensvurdering, bør den dataansvarlige rådføre seg med personvernombudet.

Hvis virksomheten ikke har personvernombud (PVO), kan dette beskrives her.

### B 3. Personvernombudets anbefaling og når denne ble gitt

Personvernombudets anbefaling, samt dato for anbefaling oppgis her.

Dersom vurderingen er et eget dokument, legg til i lista over vedlegg.

Hvis virksomheten ikke har personvernombud (PVO), kan dette beskrives her.

### B 4. Det er besluttet at

På bakgrunn av punktene over tar virksomheten stilling til om det skal gjennomføres en personvernkonsekvensvurdering.

[20] Les mer om dette her https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-er-risiko-hoy/

### B 5. Beskriv hvorfor det skal/ikke skal gjennomføres en personvernkonsekvensvurdering

Her skal virksomheten dokumentere sin beslutning.

Ledelsen skal dokumentere begrunnelsen og den skal signeres av den som har myndighet til å treffe beslutningen. Personvernforordningen definerer ikke hvilket ledelsesnivå som skal eller bør ta beslutningen. Det kan være hensiktsmessig å følge virksomhetens eksisterende rutiner og retningslinjer for risikostyring på andre områder.

Det er viktig å dokumentere godt dersom virksomheten har kommet frem til at det ikke skal gjennomføres en personvernkonsekvensvurdering og hvorfor behandlingen ikke vil medføre spesielt høy risiko. Dette er særlig viktig dersom ett eller flere av kriteriene i Artikkel 29-gruppens veileder er oppfylt, men vurderingen er at risikoen ikke er høy.

Å beskrive momentene som etter virksomhetens vurdering krever en personvernkonsekvensvurdering, vil kunne være nyttig i det videre arbeidet med personvernkonsekvensvurderingen. Beskrivelsen vil hjelpe virksomheten til å konkretisere og fokusere på de risikoene som ble identifisert i den innledende «Behovsvurderingen».

Begge typer begrunnelse kan virksomheten vise til hvis det skulle være nødvendig på et senere tidspunkt.

Dersom virksomheten ønsker å gjennomføre en personvernkonsekvensvurdering selv om det ikke er nødvendig, kan dette også beskrives her. Det er i så fall viktig at virksomheten ikke krysser av for noen av avkrysningsmulighetene.

# C. Beskrivelse av behandlingen av personopplysninger

Her skal virksomheten gi en detaljert beskrivelse av den planlagte behandlingen av personopplysninger. Vurderingen av personvernkonsekvenser skal ikke gjøres før del D.

På denne måten viser virksomheten også til hvordan og hvorfor den har kommet frem til resultatet. Virksomheten skal vise til hvilke vilkår eller krav som er oppfylt, men også hvilke faktiske forhold personvernkonsekvensvurderingen bygger på.

Virksomheten kan fylle ut denne delen både før og etter at den har gjort vurderingen som dokumenteres i del B. Virksomheten kan når som helst gå tilbake til denne delen av dokumentet for å fylle ut ytterligere informasjon der det er nødvendig.

### C 1. Det overordnede formålet med behandlingen av personopplysninger er

Her skal virksomheten angi hva som er formålet med den planlagte behandlingen av personopplysninger. Det kan være lurt å ta utgangspunkt i hva virksomheten ønsker å oppnå med behandlingen.

For mer informasjon om fastsettelse av formål, se Datatilsynet[21] og Normens faktaark Formål og behandlingsgrunnlag[22].

### C 2. Hvem er de registrerte? Beskriv hvilke kategorier.

Her skal virksomheten oppgi hvilke kategorier av registrerte som det skal behandles opplysninger om. Dette kan for eksempel være pasienter, ansatte, besøkende, helsepersonell og andre helseaktører, kontaktpersoner hos samarbeidspartnere, innleide konsulenter og innbyggere i en innbyggerundersøkelse.

### C 3. Hører noen av de registrerte til en sårbar gruppe?

I oversikten skal det angis hvem som kan betegnes som en sårbar gruppe. Oversikten er ikke uttømmende.

Eksempler på sårbare registrerte er barn og pasienter/brukere. Barn har redusert evne til å motsette seg eller gi samtykke til behandling av personopplysninger. Pasienter/brukere anses som sårbare da vedkommende står i et avhengighetsforhold til dataansvarlig/virksomheten.

Dersom virksomheten identifiserer flere som kan betegnes som sårbar gruppe og denne ikke er omfattet av den oppgitte oversikten, kan dette føres opp i punktet «andre».

[21] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/fastsette-formal/
[22] https://www.ehelse.no/normen/faktaark/faktaark-56--formal-og-behandlingsgrunnlag

### C 4. Beskriv hvorfor de registrerte er sårbare:

Virksomheten skal beskrive hvorfor de registrerte er sårbare. Er det et avhengighetsforhold mellom de registrerte og dataansvarlig? Er det for eksempel en skjevhet i maktforholdet mellom den registrerte og den virksomheten eller personen som ber den registrerte om samtykke?

Dersom det er skjevheter i maktforholdet, bør det komme frem i dette punktet.

Et eksempel på skjevheter i maktforholdet er dersom den registrerte ikke har samtykkekompetanse.

### C 5. Beskriv hvor mange registrerte som vil få sine personopplysninger behandlet

Her skal virksomheten angi et omtrentlig antall over mengden av registrerte som vil få sine personopplysninger behandlet.

For eksempel er det 100 pasienter det skal registreres opplysninger om eller er det 10 % av 100 pasienter?

### C 6. Beskriv hvordan personopplysningene vil bli håndtert (dataflyten) i den planlagte behandlingen av personopplysninger

En god beskrivelse av dataflyten vil være nødvendig for å få frem detaljene i den planlagte behandlingen av personopplysninger.

Virksomheten skal beskrive/illustrere hvor personopplysningene er hentet fra, hvordan de innhentes, hvordan de lagres videre, lagringstid, om de sammenstilles med andre opplysninger, hvem som til enhver tid har tilgang til opplysningene, hvordan de benyttes og forvaltes videre eller slettes, samt om opplysningene utleveres til tredjeparter.

Dersom det er hensiktsmessig, kan beskrivelsen av dataflyt deles inn etter behandlingsaktivitet.

Virksomheten bør bl.a. få frem hvilke nettverk, enheter og verktøy som skal brukes. Geografisk omfang bør også belyses, herunder om opplysninger overføres til land i eller utenfor EU og EØS. Se også punktet om leverandører.

På dette punktet kan dialog med leverandører og databehandlere være nyttig.

Legg gjerne med flytskjema ol i listen over vedlegg. Et eventuelt flytskjema kan lages med enkle figurer i Microsoft Word eller PowerPoint eller med spesielle verktøy for flytskjema.

### C 7. Beskriv bruk av leverandører (inkludert databehandlere) og relasjonen til disse

Her skal virksomheten gi en oversikt over alle leverandører den benytter seg av i forbindelse med behandlingen av personopplysninger, inkludert underleverandører/ underdatabehandlere. Leverandørers roller og hvilket arbeid de skal utføre kan beskrives i dette punktet. Det kan også legges inn referanser til innhold i avtaler dersom det er relevant for vurderingen.

Ved overføring av personopplysninger til land utenfor EU/EØS må virksomheten ha et gyldig overføringsgrunnlag etter personvernforordningen. Hvis den har et slikt grunnlag, kan det oppgis her.

Bruk av leverandører eller underleverandører kan medføre en forhøyet risiko dersom disse er etablert eller yter tjenester fra områder utenfor EU/EØS.[23]

Legg gjerne med avtaler o.l. i listen over vedlegg.

### C 8. Andre momenter som er relevante for personvernkonsekvensvurderingen

Bruk av teknologi som er ny for virksomheten kan føre til nye former for innsamling og bruk av personopplysninger med høy risiko for den enkeltes rettigheter og friheter. Det samme gjelder behandlinger der mange aktører er involvert, og der fordelingen av ansvar mellom flere aktører er komplisert eller uklar.

Her kan virksomheten blant annet beskrive hvordan den bruker verktøy og tekniske løsninger, og hvilke deler av behandlingen dette gjelder. Det bør for eksempel legges inn slike beskrivelser dersom virksomheten benytter profilering, automatisk innhenting av personopplysninger, mellomlagring, automatiske avgjørelser, kunstig intelligens eller teknologi som er ny for virksomheten. Virksomheten bør utdype hvordan verktøyene/løsningene vil bli brukt, hvordan verktøyene/løsningene er tilpasset situasjonen (konfigurert) og hvilke tiltak virksomheten har iverksatt for å ta vare på de registrertes interesser (garantier). Andre forhold som kan være relevante å beskrive er status på den tekniske utviklingen på området eller om det har vært sikkerhetsproblemer forbundet med teknologien eller behandlingen tidligere.

Virksomheten kan her også beskrive et eventuelt felles dataansvar og hvordan dette er organisert. Se også om felles dataansvar i del A.

### C 9. Beskriv hvordan de generelle personvernprinsippene er ivaretatt

Her skal virksomheten beskrive hvordan de sørger for å opptre i tråd med de generelle personvernprinsippene.

Personvernprinsippene deles inn følgende kategorier:

- Lovlighet, rettferdighet og åpenhet
- Formålsbegrensning
- Dataminimering
- Riktighet
- Lagringsbegrensning
- Integritet og konfidensialitet
- Ansvarlighet

For mer om innholdet i de ulike rettighetene, se Datatilsynet[24] og Normens faktaark Personvernprinsippene[25]. I Datatilsynets veiledning finnes også informasjon om eventuelle unntak fra plikten til å oppfylle rettighetene.

[23] https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/retningslinjer-og-uttalelser-fra-personvernradet/utfyllende-veiledning-om-schrems-ii/
[24] https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/
[25] https://www.ehelse.no/normen/faktaark/faktaaark-57-personvernprinsippene

Dersom det er utarbeidet rutiner og retningslinjer for ivaretakelse av prinsippene, bør virksomheten vise til disse. Det er også mulig å legge ved rutinene som vedlegg.

### C 10. Beskriv hvordan de registrertes rettigheter er ivaretatt

Her skal virksomheten beskrive hvordan de registrertes rettigheter skal ivaretas.

De registrertes rettigheter er:

- Retten til informasjon om behandlingen av personopplysninger
- Retten til innsyn
- Retten til retting
- Retten til sletting
- Retten til å kreve begrenset behandling av personopplysninger
- Retten til dataportabilitet
- Retten til å protestere mot behandling av personopplysninger
- Rettigheter ved automatiserte avgjørelser

For mer om innholdet i de ulike rettighetene, se Datatilsynet[26] og Normens Veileder for rettigheter ved behandling av helse- og personopplysninger[27]. I veilederen finnes også informasjon om eventuelle unntak fra plikten til å oppfylle rettighetene.

Dersom det er utarbeidet rutiner og retningslinjer for ivaretakelse av rettighetene, bør virksomheten vise til disse. Det er også mulig å legge ved rutinene som vedlegg.

Eksempler på utfylling:

| |
|---|
| Retten til innsyn: Den registrerte kan logge seg inn på «Min side» ved bruk av Bank-ID. Vedkommende har tilgang til alle opplysninger som er registrert om ham/henne. Virksomheten har i tillegg manuell rutine for innsyn, se arkivreferanse x/xx (versjon 3.0). |

### C 11 Hvordan er kravet til innbygd personvern ivaretatt?

Feltet skal brukes når vurderingen gjelder utvikling eller innkjøp av et IT-system eller en løsning som skal brukes i behandling av personopplysninger. Feltet kan også brukes i andre tilfeller der det er relevant å belyse hvordan innebygd personvern påvirker risikobildet. Siden det er en nær sammenheng mellom innebygd personvern og hvordan virksomheten sikrer ivaretakelse av personvernprinsippene og de registrertes rettigheter, så bør dette feltet ses i sammenheng med feltene før.

Innebygd personvern og personvern som standardinnstilling er krav i personvernregelverket. Målet er å sikre at personvernet ivaretas i alle faser et system eller en løsning gjennomgår, helt fra utvikling til drift og forvaltning. Ved å bygge inn personvernet i løsninger, systemer

[26] https://www.datatilsynet.no/rettigheter-og-plikter/den-registrertes-rettigheter/
27 https://www.ehelse.no/normen/veiledere/veileder-for-rettigheter-ved-behandling-av-helse-og-personopplysninger

eller programvare som benyttes i forbindelse med behandling av personopplysninger, kan virksomheten sørge for etterlevelse av personvernprinsipper og ivaretakelse av de registrertes rettigheter. Det kan være aktuelt å bruke innebygd personvern som et krav til arbeidsmetode og innhold i forbindelse med utvikling av IT-systemer og -løsninger. Det kan også være aktuelt å bruke innebygd personvern til å utarbeide kravspesifikasjonen i en anskaffelse av et IT-system eller en løsning.[28]

[28] Du kan lese mer om innebygd personvern i https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/programvareutvikling-med-innebygd-personvern/

# D. Vurdering av personvernkonsekvenser

I del D i malen er det de konkrete vurderingene av risikoer og tiltak som er avgjørende å få frem og dokumentere. Dette skal ikke være en beskrivelse av hvordan behandlingen er tenkt gjennomført (det dokumenteres i del C). Vurderingen av personvernkonsekvenser handler ikke om hvilken risiko virksomheten løper på egne vegne, men hvilke risikoer, i et personvernperspektiv, behandlingen av personopplysninger innebærer og hvilke konsekvenser behandlingen kan medføre for enkeltpersonene virksomheten behandler opplysninger om. Eventuelt hvordan behandlingen kan påvirke andre fysiske personer.

Når virksomheten starter på en personvernkonsekvensvurdering fordi den har identifisert at **risikoen for personvernet er høy (i del B)**, må den være innstilt på å gjøre endringer/tilpasninger i den planlagte behandlingen av personopplysninger. Det er ikke nødvendigvis mulig å redusere samtlige identifiserte risikoer. Virksomheten må ha som mål å bringe risikoen til et akseptabelt nivå. Alternativet er forhåndsdrøfting med Datatilsynet eller at behandlingen ikke kan gjennomføres.

**Hvordan skal virksomheten gå frem?**

For at personvernkonsekvensvurderingen skal være hensiktsmessig, fokusert og tydelig med tanke på hva virksomheten mener vil innebære høy risiko og hvordan dette kan håndteres, vil det være lurt å ta utgangspunkt i de forholdene som utløste behovet for en personvernkonsekvensvurdering. Gå derfor tilbake til del B i malen, og se på vurderingene og konklusjonene.

Hvilke aspekter ved den planlagte behandlingen innebærer en økt risiko for de registrerte og hvorfor?

Mange virksomheter har gode rutiner for risiko- og sårbarhetsvurderinger av informasjonssikkerheten. Dersom det er utført en slik vurdering for en relevant aktivitet eller system som inngår i behandlingen av personopplysninger, vil disse vurderingene være viktige å få med i personvernkonsekvensvurderingen.

### D 1. Beskriv hvorfor behandlingen av personopplysninger er nødvendig for å ivareta formålet

Her skal virksomheten beskrive hvorfor det er nødvendig å behandle personopplysningene for å kunne gjennomføre det overordnede formålet. En slik nødvendighetsvurdering skal alltid gjøres, uavhengig av om behandlingen krever en personvernkonsekvensvurdering etter artikkel 35. Det bør gjøres en ny vurdering av dette i forbindelse med personvernkonsekvensvurderingen fordi målet er å komme frem til tiltak som kan redusere den høye risikoen virksomheten har identifisert. I dette ligger også at virksomheten på nytt vurderer om personvernprinsippene oppfylles.

Når den vurderingen gjøres tar virksomheten stilling til om måten behandlingen skal skje på vil oppfylle personvernprinsippene og om valgene står i et rimelig forhold til formålet med behandlingen.

For mer veiledning om hvordan virksomheten konkret kan gå frem for å gjøre dette, se Datatilsynets sjekkliste[29] for vurdering av personvernkonsekvenser (del 2. om nødvendighet og proporsjonalitet), samt Normens Faktaark om personvernprinsippene[30].

Ta utgangspunkt i det dere allerede har fylt ut i malen. Der skal dere ha redegjort for ulike aktiviteter, tilhørende formål og tatt stilling til behandlingsgrunnlag.

**D 2. Beskriv hvorfor det ikke vil være mulig å ivareta formålene på en mindre inngripende måte (f.eks. med færre/ingen personopplysninger, uten bruk av inngripende teknologi eller lignende)**

Her skal virksomheten, med utgangspunkt i de identifiserte momentene i del B i malen, begrunne hvorfor og hvordan mindre inngripende måter å gjennomføre behandlingen på vil gjøre det vanskelig å oppnå formålene. Dette punktet skal være med på å understøtte vurderingen av om behandlingen er nødvendig for å ivareta formålet.

For eksempel:

- Hvorfor er det ikke tilstrekkelig å behandle personopplysninger om et mindre antall personer?
- Hvorfor kan formålet ikke oppnås uten særlige kategorier personopplysninger/helseopplysninger?
- Hvorfor må behandlingen pågå over så lang tid?
- Hvorfor er det nødvendig for flere å ha tilgang til opplysningene?

**D 3. Beskriv hvilke risikoer for de registrertes rettigheter og friheter virksomheten har identifisert**

Her skal virksomheten beskrive de identifiserte risikoene for de registrertes rettigheter og friheter. Vurderingene som gjøres i en personvernkonsekvensvurdering skal ta utgangspunkt i den registrertes perspektiv, i motsetning til tradisjonelle risikovurderinger som benytter virksomhetsperspektivet. En personvernkonsekvensvurdering kan gjøres i forkant, samtidig og/eller i etterkant av en risikovurdering av informasjonssikkerheten. Disse vurderingene må ses sammenheng. Den vurderingen som ferdigstilles først må oppdateres etter at den andre er ferdig, for å sikre at alle relevante risikomomenter er ivaretatt.

En personvernkonsekvensvurdering kan gjennomføres og dokumenteres på ulike måter. Dersom virksomheten har etablert en annen metode for risikovurderinger enn den som fremgår av tabellen i malen, er det ingenting i veien for at en benytter den etablerte metoden i virksomheten. Personvernperspektivet må være del av metoden en benytter.

Eksempler på mulige risikoer:

- Manglende reell medbestemmelse, herunder manglende frihet ved bruk av samtykke i arbeidsforhold

[29] https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/dpia-veileder/sjekkliste-for-dpiafaser.pdf
[30] https://www.ehelse.no/normen/faktaark/faktaaark-57-personvernprinsippene

- Manglende reell åpenhet, f.eks. ved at den registrerte ikke får informasjon om behandlingen av personopplysninger, eller at informasjonen er misvisende/mangelfull
- Manglende forutsigbarhet, som blant annet innebærer at den registrerte må få informasjon om behandlingen og hva den innebærer. Forutsigbarhet knyttes gjerne til personvernprinsippet om rettferdighet, og et eksempel på situasjon hvor forutsigbarheten kan være begrenset, er ved automatiserte avgjørelser.
- Svekkelse av opplysningenes integritet eller redusert/manglende konfidensialitet
- Ikke mulighet for innsyn
- Ikke mulighet for retting og/ eller sletting
- Ikke mulighet til å protestere på behandlingen av personopplysninger
- Brudd på retten til å ikke bli diskriminert
- Brudd på retten til ytringsfrihet og religionsfrihet

**Beskriv/ konkretiser hvilke risikomomenter som er vektlagt i risikovurderingen**

Virksomheten skal vurdere om behandlingen av personopplysninger innebærer at personvernprinsippene ikke etterleves, eller om den enkeltes rettigheter eller friheter vil stå i fare for å ikke kunne innfris. De registrertes rettigheter og friheter omfatter de rettighetene som følger av personvernforordningen kapittel 3, men også helserettigheter og andre grunnleggende menneskerettigheter som retten til privatliv, kommunikasjonsvern, ytringsfrihet, tankefrihet, bevegelsesfrihet, forbud mot diskriminering. Retten til frihet og samvittighets- og religionsfrihet er også rettigheter og friheter som må tas med i vurderingen av hvilke konsekvenser behandlingen av personopplysninger kan få for den registrerte.

Dette innebærer at, i tillegg til mangel på etterlevelse av personvernprinsippene eller at den registrertes rettigheter og friheter ikke kan innfris, kan behandlingen av personopplysninger også lede til andre/ytterligere konsekvenser for den registrerte (se eksempler på mulige konsekvenser i listen under). Dersom det identifiseres risikoer som ikke er relatert til personvernet, er det momenter som kan løftes frem, men hvor vurderinger/avveininger bør håndteres i forbindelse med ledelsens beslutning.

Ta utgangspunkt i risikoene under, og eventuelt andre identifiserte risikoer, og før den enkelte risiko opp i tabellen i malen. Virksomheten må kopiere og lime inn tabellen i malen så mange ganger det er nødvendig for å få beskrevet alle aktuelle risikoer for de registrertes rettigheter og friheter.

Eksempler på mulige konsekvenser for rettigheter og friheter som kan følge av risikoene over

- forskjellsbehandling
- identitetstyveri eller -bedrageri
- økonomisk tap
- skade på omdømme for den registrerte
- Brudd på taushetsplikten
- Tap av tillit
- uautorisert oppheving av pseudonymisering[31]
- økonomiske eller sosiale ulemper

[31] Les mer om dette her https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/hvordan-anonymisere-personopplysninger/

- manglende tilgang på helse- og omsorgstjenester
- Fare for liv, helse, (f.eks. dersom viktige helseopplysninger ikke er tilgjengelige for de som har behov for dem)
- nedsatt livskvalitet (f.eks. dersom behandlingen utløser bekymring hos den registrerte)
- Risiko for krenkelse av integritet/integritetstap
- Subjektiv belastning for den enkelte
- Konsekvenser knyttet til feil diagnose
- Misinformasjon, redsel knyttet til f.eks. misforstått diagnose
- Tap av tillit til den dataansvarlige/helseforetaket
- personopplysningene brukes til andre formål

Før virksomheten fyller ut tabellen, en tabell pr risiko, er det viktig å sjekke hvilke rettigheter som følger av behandlingsgrunnlaget for den aktuelle behandlingsaktiviteten/delformålet. Den registrerte har for eksempel ikke rett til dataportabilitet, med mindre behandlingsgrunnlaget er samtykke eller avtale.

Det er utarbeidet et alternativ til tabellen i malen, hvor samtlige identifiserte risikoer/risikoscenarier kan listes opp og vurderes i en og samme tabell i Excel-format. Excel-tabellen ligger som vedlegg til malen. I samme skjema ligger mal for en tiltaksliste som vil gi oversikt over tiltak, risiko før/ etter tiltak og tiltakseier.

| Punkt i malen | Veiledning til utfylling |
|---|---|
| | |
| Beskriv risikoen for fysiske personers rettigheter eller friheter, som kan oppstå (risikoscenario): | Ta utgangspunkt i risikoene i listen over og ev. andre identifiserte risikoer. Resten av tabellen gjelder den konkrete risikoen virksomheten fører opp her. Som tidligere beskrevet må derfor selve tabellen kopieres og fylles ut helt til alle identifiserte risikoer er vurdert. |
| Hvilke(n) behandlingsaktivitet(er) er risikoen relatert til: | Her bør behandlingen brytes ned til hensiktsmessige delaktiviteter, relevant for risikoen det er snakk om. Dette kan for eksempel være risikoen for at opplysninger gjøres tilgjengelig for andre enn de som skal ha tilgang, fordi de må overføres fra f.eks. pasientjournal til sikker database via et nettverk. Vær oppmerksom på at det kan være risikoer som gjelder flere ulike behandlingsaktiviteter, men hvor konsekvensene vil være ulike. Et eksempel kan være at risikoen for forskjellsbehandling vil kunne være større ved prosessering av data gjennom automatisk saksbehandling. |
| Beskriv hvor sannsynlig det er at risikoen oppstår: | Sannsynlighet kan beskrives på ulike måter. Det kan gjøres ved å anslå hendelsesintervaller/hyppighet (hendelsen inntreffer daglig, ukentlig, flere ganger i året, sjeldnere), eller ved å dele sannsynlighet inn i lav, middels og høy. Virksomheten kan benytte den metodikken som den benytter ved vanlige ROS-analyser, dersom den synes å treffe godt med tanke på behandlingsaktiviteten. |
| Beskriv hvilke konsekvenser dette kan få for den registrerte: | Hva kan hendelsen resultere i for den enkelte registrerte? Personvernprinsippene kan være nyttig å bruke for å identifisere konsekvenser. Dersom virksomheten for eksempel har identifisert en |

| | | | |
|---|---|---|---|
| | risiko for at personopplysninger gjøres tilgjengelig for uvedkommende, vil dette kunne relateres til personvernprinsippet om konfidensialitet og tilgjengelighet. | | |
| Beskriv eksisterende tiltak som reduserer risikoen: | Hvilke tekniske eller organisatoriske grep har virksomheten innført for å dempe risikoen? Organisatoriske grep kan f.eks. være rutiner og retningslinjer (husk å beskrive disse), samt oppfølging og kontroll av at disse følges. Et eksempel på tekniske tiltak kan være tilgangskontroll. Å beskrive eksisterende tiltak kan også være aktuelt i forbindelse med pågående behandlinger av personopplysninger hvor tiltak kan videreføres. | | |
| Beskriv virksomhetens vurdering av om risikoen er akseptabel: | Her må virksomheten gjøre en konkret vurdering av om dette er en risiko som kan aksepteres. Virksomheten skal ha retningslinjer for hva som anses som akseptabel risiko.<br><br>Eksempel på vurdering: Automatisert behandling av personopplysninger kan gi gevinster i form av redusert saksbehandlingstid slik at flere pasienter mottar et vedtak. I tillegg kan automatisert behandling redusere faren for menneskelige feil som er påvist ved den manuelle saksbehandlingen.<br>Ved automatisert behandling er det identifisert en viss risiko for feil vedtak. Risikoen for feil vedtak følger av at automatisert behandling øker risikoen for at uriktige opplysninger ikke oppdages og på denne måten fører til feil beslutning. Virksomheten har funnet at andelen feil ved manuell saksbehandling er høyere enn hva man kan forvente ved automatisert saksbehandling.<br>Virksomhetens ledelse stiller følgende spørsmål: Kan vi som virksomhet, på bakgrunn av dette, akseptere sannsynligheten for at 10 personer per år får feil vedtak fordi personopplysningene deres behandles automatisk, gitt at vi har innført tiltak x, z og y som skal redusere/motvirke risikoen? | | |
| Beskriv planlagte tiltak som reduserer risikoen : | Dersom den eksisterende risikoen ikke kan aksepteres, må virksomheten redegjøre for ytterligere tiltak. Virksomheten må også redegjøre for hvordan tiltakene vil redusere risikoen. | | |
| Ansvarlig for tiltak: | | Frist: | |

**D 4 .Oppsummering av konsekvensvurderingen**

Her skal virksomheten oppsummere det som samlet fremgår av tabellene hvor risikoene og tiltak er beskrevet. Her kan det være viktig få frem hva som er vektlagt og hvilke hensyn som spiller inn. En slik oppsummerende beskrivelse av identifiserte risikoer og tiltak vil gjøre det lettere for beslutningstakere å ta stilling til om personvernkonsekvensvurderingen er dekkende.

Eksempel på utfylt tabell:

| **Beskriv risikoen for fysiske personers rettigheter eller friheter, som kan oppstå (risikoscenario):** | | | |
|---|---|---|---|
| Manglende reell åpenhet | | | |
| **Hvilke(n) behandlingsaktivitet(er) er risikoen relatert til:** | Opplysninger om et stort antall personer skal utleveres fra et sentralt helseregister. Det gis ikke individuell informasjon om behandlingen av personopplysninger til de registrerte, da det vil være umulig/vil innebære uforholdsmessig stor innsats å kontakte så mange registrerte, jf. unntaksbestemmelse i personvernforordningen (Art. 14, punkt 5, bokstav b). | | |
| **Beskriv hvor sannsynlig det er at risikoen oppstår:** | Sannsynlig, da ingen mottar individuell informasjon. | | |
| **Beskriv hvilke konsekvenser dette kan få for den registrerte:** | At de registrerte ikke mottar informasjon om behandlingen innebærer at de ikke blir kjent med at personopplysninger om dem behandles til det konkrete formålet (vitenskapelig forskning), og de vil derfor heller ikke gjøres kjent med eller være i stand til å benyttes seg av sine øvrige rettigheter. | | |
| **Beskriv eksisterende tiltak som reduserer risikoen:** | Unntaksbestemmelsen i personvernforordningen stiller krav om at den dataansvarlige ved bruk av unntaksbestemmelsen plikter å treffe egnede tiltak for å verne den registrertes rettigheter og friheter og berettigede interesser, herunder gjøre informasjonen offentlig tilgjengelig. Virksomheten finner ikke egnede tiltak som kan redusere risikoen i tilstrekkelig grad, da de verken kan redusere omfang eller detaljgrad på opplysningene de trenger uten at dette i vesentlig grad svekker forskningsprosjektet. Virksomheten har planlagt å offentliggjøre informasjon om forskningsprosjektet på forskningsinstitusjonens nettsider. | | |
| **Beskriv virksomhetens vurdering av om risikoen er akseptabel:** | Virksomheten mener at risikoen ikke er akseptabel, da det er sannsynlig at informasjon på egen nettside ikke vil nå særlig mange av de registrerte. Mangel på informasjon påvirker de registrertes mulighet til å benytte sine øvrige rettigheter. I vurderingen har virksomheten vektlagt at personvernulempen er høy fordi detaljgraden på opplysningene som er nødvendige er stor, og at enkeltpersoner kan identifiseres i datamaterialet. | | |
| **Beskriv planlagte tiltak som reduserer risikoen :** | Virksomheten beslutter at offentlig informasjon fra deres egne nettsider ikke vil oppfylle målet om å nå de registrerte. Følgende tiltak skal iverksettes for å redusere risikoen for manglende reell åpenhet: Virksomheten vil utarbeide informasjonsskriv og tekst til nettsider som de vil be relevante pasientorganisasjoner spre/publisere. | | |
| **Ansvarlig for tiltak:** | | Frist: | |

# E. Innspill og ledelsens beslutning

Her skal virksomheten dokumentere hvilke innspill den har fått fra registrerte og/eller representanter for de registrerte, innspill fra personvernombudet og eventuelle andre aktører. Til slutt skal virksomheten dokumentere beslutningene den har tatt etter at den har gjennomført vurderingen av personvernkonsekvenser.

### E 1. Innspill fra registrerte eller representanter for de registrerte[32]

Her skal virksomheten beskrive om den har innhentet innspill fra den registrerte eller representanter for den registrerte og hvilke innspill som er kommet. Å innhente innspill fra de registrerte eller deres representanter kan ofte være hensiktsmessig, men det kan også ofte være påkrevd i henhold til personvernforordningen artikkel 35 nr. 9.

Representanter for de registrerte kan være et utvalg brukere/pasienter, pårørendeorganisasjon, pasientombud, eldreråd, eller andre som vil få sine personopplysninger behandlet i behandlingen som personvernkonsekvensvurderingen tar for seg.

Innspill fra den registrerte kan innhentes på flere måter, for eksempel ved å delta i selve vurderingen av personvernkonsekvenser sammen med virksomheten, eller sende inn skriftlige innspill til dataansvarlig. Dersom de registrerte er deltagere i selve vurderingen av personvernkonsekvenser (malens del D), skal de også oppføres som deltakere.

Det er viktig at virksomheten gir den registrerte som gir innspill eller deltar i vurderingen god nok forståelse for behandlingen. Dette skal sikre at innspillene fra den registrerte i størst mulig grad omhandler de relevante forholdene rundt behandlingen og hvordan den registrerte oppfatter at personvernet blir ivaretatt. Virksomheten kan stille spørsmål til den registrerte om forventninger til behandlingen, for eksempel knyttet til hva slags informasjon som bør gis, og den beste måten å gi den på. Dette er særlig viktig hvis de registrerte er en sårbar gruppe, for eksempel barn, pasienter, personer uten samtykkekompetanse og personer med et annet morsmål.

Virksomheten bør også dokumentere om innspillene til de registrerte har blitt tatt til følge eller ikke, for eksempel om de har resultert i at ekstra tiltak for å redusere en risiko har blitt innført, eller at en rutine for å oppfylle rettigheter har blitt endret.

### E 2. Dersom det ikke har vært mulig å få innspill fra de registrerte, beskriv hvorfor:

Dersom virksomheten har forsøkt å innhente innspill uten å lykkes eller ikke har bedt om innspill, skal dette forklares/begrunnes.

### E 3. Anbefalinger fra personvernombudet

Her skal virksomheten dokumentere hvilke anbefalinger/merknader personvernombudet har gitt *etter* at malens del D – vurdering av personvernkonsekvenser er fylt ut. I henhold til personvernforordningen artikkel 39 1. bokstav c skal personvernombudet kontrollere

[32] Dersom virksomheten har mottatt flere innspill, så må virksomheten kopiere og lime inn skjemaet under så mange ganger det er nødvendig for å få redegjort for alle innspillene.

gjennomføringen av personvernkonsekvensvurderingen. Dette innebærer at ombudet i etterkant av vurderingen skal kontrollere at den dekker minimumskravene i personvernforordningen artikkel 35, og eventuelt komme med egne merknader til de enkelte vurderingene som virksomheten har gjennomført.

Det kan for eksempel være aktuelt for personvernombudet å påpeke risikoer som ikke har blitt vurdert eller andre mangler som bør utbedres før ledelsen tar stilling til risikoen. Personvernombudet kan også være uenig i vurderinger som virksomheten har gjort, og dette bør alltid dokumenteres og presenteres for ledelsen sammen med personvernkonsekvensvurderingen.

Dersom vurderingen er et eget dokument, legg til i lista over vedlegg.

### E 4. Innspill fra andre

Dersom virksomheten har interne rutiner for å innhente innspill fra andre enn de registrerte/representanter for de registrerte og personvernombudet, kan dette beskrives her. Aktuelle aktører kan for eksempel være helsefaglige råd, sikkerhets-/personvernforum, etisk råd o.l. Dette feltet kan også benyttes dersom prosjektleder ønsker å gi et oppsummerende innspill til ledelsens beslutning.

### E 5. Ledelsens beslutning etter at personvernkonsekvensvurderingen er gjennomført

Når vurderingen av personvernkonsekvenser er gjennomført, vil virksomheten stå igjen med en restrisiko som ledelsen skal ta stilling til. Denne restrisikoen skal ledelsen kunne få en klar oppfatning av ved å gjennomgå vurderingen som er gjort i del D i malen. Personvernforordningen sier at man skal ha en risikobasert tilnærming til arbeidet med personvern. Dette betyr at virksomheten må sette inn ressurser der risikoen er antatt eller påvist å være størst. Det anbefales at oppfølgingen av foreslåtte tiltak som fremgår av tabellen(e), inkluderes i virksomhetens etablerte internkontrollarbeid.

Basert på restrisikoen skal ledelsen beslutte om de vil akseptere risikoen og gjennomføre behandlingen. Om restrisikoen er for høy kan ledelsen beslutte at behandlingen ikke skal gjennomføres. Dersom risikoen er for høy, må ytterligere tiltak implementeres og dokumenteres før ledelsen igjen tar stilling til om behandlingen kan gjennomføres. Dersom ledelsen fremdeles ikke aksepterer risikoen, men allikevel ønsker å gjennomføre behandlingen, må det gjennomføres forhåndsdrøfting med Datatilsynet.[33]

De som har utført selve personvernkonsekvensvurderingen og lagt den frem for ledelsen for en beslutning, har som regel utelukkende hatt personvern som fokus for sin vurdering. Virksomhetens samfunnsoppdrag og målsetninger vil innebære at ledelsen veier ulike hensyn opp mot hverandre, og det er viktig at ledelsen inkluderer andre hensyn enn personvern i sin beslutning der dette er relevant.

Ledelsen skal dokumentere begrunnelsen skriftlig, og den skal signeres av den som har myndighet til å treffe beslutningen. Personvernforordningen definerer ikke hvilket ledelsesnivå som skal eller bør ta beslutningen. Det kan være hensiktsmessig å følge virksomhetens eksisterende rutiner og retningslinjer for risikostyring på andre områder.

[33] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/forhandsdroftelser/

Til slutt bør det besluttes når personvernkonsekvensvurderingen skal gjennomgås og eventuelt revideres, samt hvem som har ansvaret for gjennomføring. Dette bør gjøres med jevne mellomrom, for eksempel en gang i året. Legg merke til at dette er planlagte gjennomganger. Gjennomganger eller revisjoner som følge av avvik eller endringer i risikobildet kommer i tillegg, og skal dokumenteres.

Direktoratet for e-helse

**Besøksadresse**
Verkstedveien 1
0277 Oslo

**Postadresse**
Postboks 6737
St. Olavs plass