Direktoratet for e-helse

Mal for personvern-konsekvensvurdering (DPIA) med veiledning til utfylling

HITR 1243:2021

Publikasjonens tittel:
Mal for personvernkonsekvensvurdering med veiledning til utfylling

Rapportnummer
HITR 1243:2021

Utgitt:
[Sett inn dato]

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Publikasjonen kan lastes ned på:
www.ehelse.no

Innhold

Om malen og veilederen

Bakgrunn

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

En vurdering av personvernkonsekvenser (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. Den dataansvarlige skal gjøre en slik personvernkonsekvensvurdering hvis det er sannsynlig at en behandling medfører høy risiko for de registrerte.

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[1].

Personvernkonsekvensvurderinger skal minst inneholde:

- en systematisk beskrivelse av behandlingsaktivitetene av helse- og personopplysninger
- beskrivelse av formålet med behandlingen av personopplysninger
- 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.

Dataansvarlige i helse- og omsorgssektoren behandler ofte 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. Dataansvarlige i sektoren er også ofte involvert i forskningsprosjekter 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 en plikt til å utføre personvernkonsekvensvurdering. For å gi dataansvarlige i sektoren verktøy og støtte som

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

underbygger denne prosessen, har Direktoratet for e-helse videreutviklet den tidligere Mal for DPIA.

Dette indikerer at dataansvarlige i sektoren har et særskilt behov for gode verktøy og støtte som underbygger denne prosessen.

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.

Det overordnede målet med denne veilederen er 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.

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. Dette vil være enklere dersom sektoren bruker en lik standard mal for personvernkonsekvensvurdering og kompetansen om når og hvordan en personvernkonsekvensvurdering skal gjennomføres er høyere.

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 syns der er vanskelig å finne 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 personvernkonsekvensvurdering. Mer om behandlingsgrunnlag hos Datatilsynet[2] og i Normens faktaark Formål og behandlingsgrunnlag[3].

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

Det anbefales å starte arbeidet med å ta ned sentrale personvernspørsmål og vurdere ivaretakelse av rettigheter og friheter så tidlig som mulig og allerede før det foreligger et

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

løsningskonsept. En slik tidlig overordnet vurdering av personvernspørsmål vil kunne fungere som underlag for å gjennomføre en personvernkonsekvensvurdering etter artikkel 35.

Om veilederen

Denne veilederen består av to deler; en mal og en veiledning til utfylling av malen.

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 sikre 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 vurderingen 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 WP29-gruppen.

Det kan være lurt å ta utgangspunkt i kriteriene fra WP29 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.

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 veilederen skal være anvendelig, uavhengig av kompetansenivå. Det vil imidlertid være varierende behov for veiledning blant virksomhetene i sektoren, både med hensyn til utfyllingen av selve malen og til gjennomføring av en personvernkonsekvensvurdering. Noen virksomheter vil nok derfor trenge ytterligere veiledning til gjennomføringen av selve personvernkonsekvensvurderingen enn det som finnes i denne malen.

Definisjoner

Nedenfor er noen viktige begrep i malen forklart. For flere forklaringer og begreper, se personvernforordningen og definisjoner i Normen[4].

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.

[4] https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren#6%20Vedlegg

DPIA-veileder utarbeidet av WP29-gruppen:
WP29 (Working Party Article 29) var 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)[5]. De er derfor en viktig kilde til hvordan personvernregelverket skal fortolkes. Etter GPDR er WP29 er erstattet av Det europeiske personvernrådet (EDPB).

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

Dataansvarlig er i helselovgivningen det samme som 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.

Helseopplysning
personopplysninger om en fysisk persons fysiske eller psykiske helse, medregnet om ytelse av helsetjenester, som gir informasjon om helsetilstand, jf. personvernforordningen artikkel 4 nr. 15

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

I denne veilederen brukes begrepet **helse- og personopplysning** som en samlebetegnelse.

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.

Virksomhet:
En juridisk person eller organisasjon som produserer varer eller tjenester. For eksempel helseforetak, helseforvaltning, kommune, sykehus, legepraksis, tannklinikk, apotek, apotekkjede, røntgeninstitutt, frittstående laboratorium, universitet, høyskole og stiftelse.

[5] https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en

Mal del A: Kjerneinformasjon

1.1 Navn på dataansvarlig virksomhet:

1.2 Hvilken rolle har virksomheten?

☐ Dataansvarlig (alene)
☐ Dataansvarlig (felles dataansvar)
Oppgi navnet på felles dataansvarlige:

1.3 Hva er navnet på prosjektet/prosessen/systemet/løsningen som vurderes?

1.4 Arkivnummer/saksnummer eller andre viktige kjennetegn for virksomheten

1.5 Deltakere i vurderingen:

Navn:	Rolle:	Kommentar:
		.

1.6 Beskriv når og hvordan personvernombudet har blitt involvert:

1.7 Versjonshistorikk:

Versjon:	Dato:	Beskrivelse av endringer:

1.8 Oversikt over samtlige vedlegg:

Nummer:	Dokumentnavn:	Kommentar:
Vedlegg 1		
Vedlegg 2		

Mal del 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.

2.1 Indikasjoner på at personvernkonsekvensvurdering må gjennomføres:

Hva taler for at en personvernkonsekvensvurdering må gjennomføres i dette tilfellet?

☐ Behandlingen er oppført i Datatilsynets liste over behandlingsaktiviteter som alltid innebærer høy risiko for de registrertes rettigheter og friheter.[6]
Velg et element.
Velg et element.
Velg et element.
Velg et element.

☐ Et av de alternative kravene i personvernforordningen artikkel 35 (3) er oppfylt.[7]
Velg et element.
Velg et element.
Velg et element.

☐ Krav i artikkel 29-gruppens veileder er oppfylt.[8]
Velg et element.
Velg et element.
Velg et element.
Velg et element.

☐ Virksomheten har etter en konkret vurdering kommet til at det sannsynligvis foreligger høy risiko for de registrertes rettigheter og friheter (legg vurderingen til i lista over vedlegg, se punkt 1.7)

☐ Virksomheten har tidligere hatt konsesjon fra Datatilsynet eller godkjenning fra REK som er datert før juli 2018.

☐ Virksomheten har tidligere utført en personvernkonsekvensvurdering og ser et behov for å oppdatere med en ny personvernkonsekvensvurdering.

[6] Trykk på «velg element» og pilen som peker ned for å velge hvilket/hvilke krav det dreier seg om.
[7] Trykk på «velg element» og pilen som peker ned for å velge hvilket/hvilke krav det dreier seg om.
[8] Trykk på «velg element» og pilen som peker ned for å velge hvilket/hvilke krav det dreier seg om.

2.2 Har personvernombudet uttalt seg i vurderingen av behovet for å gjennomføre en personvernkonsekvensvurdering?

☐ Ja ☐ Nei

Sett inn personvernombudets anbefaling og når denne ble gitt:

2.3 Virksomheten har besluttet at:

☐ Det er nødvendig å utføre en personvernkonsekvensvurdering i henhold til personvernforordningen artikkel 35 (7)

☐ Det ikke er nødvendig å utføre en personvernkonsekvensvurdering i henhold til personvernforordningen artikkel 35 (7)

2.4 Sett inn begrunnelsen for hvorfor virksomheten har kommet til at det skal/ikke skal gjennomføres en personvernkonsekvensvurdering:

Dato:	Navn på beslutningstaker:	Rolle:

Mal del C: Beskrivelse av behandlingen av personopplysninger

Her skal virksomheten gi en detaljert beskrivelse av den planlagte behandlingen av personopplysninger.[9]

3.1 Det overordnede formålet med behandlingen av personopplysninger er:

3.2 Hvem er de registrerte?

- ☐ Innbyggere
- ☐ Besøkende
- ☐ Innleide konsulenter
- ☐ Andre:
- ☐ Ansatte
- ☐ Kontaktpersoner hos samarbeidspartnere

3.3 Hører noen av de registrerte til en sårbar gruppe?

- ☐ Pasienter
- ☐ Pårørende
- ☐ Andre:
- ☐ Barn
- ☐ Deltakere i forskningsprosjekt

[9] At en personvernkonsekvensvurdering skal inneholde dette følger av personvernforordningen artikkel 35 (7) (a)

3.4 Beskriv relasjonen mellom dataansvarlig/representant for dataansvarlig og de registrerte:

3.5 Beskriv hvor mange registrerte som vil få sine personopplysninger behandlet:

3.6 Beskriv de forskjellige behandlingsaktivitetene som inngår i vurderingen.:[10]

Behandlingsaktivitet:	
Formål:	
Rettslig behandlingsgrunnlag:[11]	
Personopplysninger som benyttes:	
Særlige kategorier av personopplysninger som benyttes:	
Lagringstid:	

[10] Dersom vurderingen gjelder flere behandlingsaktiviteter, så må virksomheten kopiere og lime inn skjemaet under så mange ganger det er nødvendig for å få beskrevet alle behandlingsaktivitetene.
[11] 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.

3.7 Beskriv hvordan personopplysningene vil bli håndtert (dataflyten) i den planlagte behandlingen av personopplysninger

3.8 Utdyp forhold som ikke fremgår tydelig av beskrivelsen av dataflyt:

3.9 Beskriv bruk av leverandører (inkludert databehandlere) og relasjonen til disse:

3.10 Annen informasjon:

3.11 Hvordan vil virksomheten opptre i samsvar med de generelle personvernprinsippene om:

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

3.12 Hvordan har virksomheten planlagt at den skal ivareta de registrertes rettigheter?

Informasjonsplikten:	
Retten til innsyn:	
Retten til retting:	
Retten til sletting:	
Retten til å kreve begrensning av behandlingen:	
Retten til å protestere mot behandlingen:	
Retten til dataportabilitet:	
Rettigheter knyttet til automatiserte avgjørelser:	
Retten til å trekke tilbake et samtykke:	

3.13 Dersom behandlingen av personopplysninger gjelder et system/løsning, hvordan er personvern bygget inn?

Mal del D: Vurdering av personvernkonsekvenser

Her skal virksomheten dokumentere hvilke risikoer for de registrertes rettigheter og friheter behandlingen av personopplysninger innebærer.[12] I tillegg skal virksomheten presentere tiltakene som skal redusere identifiserte risikoer til et akseptabelt nivå.[13] Virksomheten skal også dokumentere hvorfor den mener at behandlingen av personopplysninger er nødvendig og at den står i et rimelig forhold til formålene den utføres for.[14]

4.1 Beskriv vurderingen av om behandlingen av personopplysninger er nødvendig for å ivareta formålet:

4.2 Beskriv vurderingen av om det vil være mulig å ivareta formålene på en mindre inngripende måte (f.eks. med færre/ingen personopplysninger, uten bruk av inngripende teknologi eller lignende):

[12] At en personvernkonsekvensvurdering skal inneholde dette følger av personvernforordningen artikkel 35 (7) (c)
[13] At en personvernkonsekvensvurdering skal inneholde dette følger av personvernforordningen artikkel 35 (7) (d)
[14] At en personvernkonsekvensvurdering skal inneholde dette følger av personvernforordningen artikkel 35 (7) (b)

4.3 Beskriv hvilke risikoer for de registrertes rettigheter og friheter virksomheten har identifisert:[15] [16]

Beskriv konsekvensen for fysiske personers rettigheter eller friheter, som kan oppstå:			
Hvilke(n) behandlingsaktivitet(er) er risikoen relatert til:			
Beskriv hvor sannsynlig det er at konsekvensen oppstår:			
Beskriv hvordan konsekvensen kan påvirke de registrertes rettigheter eller friheter:			
Beskriv eksisterende tiltak som reduserer risikoen:			
Beskriv virksomhetens vurdering av om risikoen er akseptabel:			
Beskriv planlagte tiltak som reduserer risikoen:			
Ansvarlig for tiltak:		Frist:	

4.4 Beskriv/konkretiser hvilke risikomomenter som er vektlagt i risikovurderingen

[15] I veilederen finner du eksempler på uønskede effekter av behandlingen som virksomheten kan ta utgangspunkt i, og aktuelle konsekvenser for den registrertes rettigheter og friheter

[16] Virksomheten må kopiere og lime inn skjemaet under så mange ganger det er nødvendig for å få beskrevet alle aktuelle risikoer for de registrertes rettigheter og friheter

Mal del E: Innspill og ledelsens beslutning

Her skal virksomheten dokumentere hvilke innspill den eventuelt har fått fra registrerte og andre interessenter. I tillegg skal den dokumentere eventuelle innspill og anbefalinger fra personvernombudet. Til slutt skal virksomheten dokumentere beslutningene den har tatt etter at den har gjennomført vurderingen av personvernkonsekvenser.

5.1 Hvilke innspill har virksomheten fått fra registrerte, representanter for de registrerte, og/eller andre interessenter?[17]

Navn:	
Relasjon mellom de registrerte/interessenten og virksomheten:	
Beskriv hvordan de registrerte/interessenten har blitt involvert:	
Innspill:	

5.2 Hvilke anbefalinger har personvernombudet gitt?

[17] 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.

5.3 Hva er ledelsens beslutning etter at personvernkonsekvensvurderingen er gjennomført?

☐ Virksomheten har funnet tiltak som reduserer risikoen for de registrertes rettigheter og friheter til et akseptabelt nivå. Virksomheten vil derfor gjennomføre behandlingen av personopplysninger når tiltakene er etablert.

☐ Virksomheten har *ikke* funnet tiltak som reduserer risikoen for de registrertes rettigheter og friheter til et akseptabelt nivå. Virksomheten vil derfor *ikke* gjennomføre behandlingen av personopplysninger.

☐ Virksomheten har *ikke* funnet tiltak som reduserer risikoen for de registrertes rettigheter og friheter til et akseptabelt nivå. Virksomheten vil derfor gjennomføre en forhåndsdrøfting med Datatilsynet før den tar en beslutning.

Begrunnelse - Hva har ledelsen lagt vekt på i sin beslutning?

Dato:	**Navn på beslutningstaker:**	**Rolle:**

Dato for neste gjennomgang av vurderingen:	Ansvarlig for neste gjennomgang av vurderingen (rolle):

Veiledning til del 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.

1.1 Navn på dataansvarlig virksomhet

Oppgi navn på dataansvarlig virksomhet.

1.2 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. 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.

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. De skal da føres opp i oversikten over deltakere, se punkt 1.5.

1.3 Hva er 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.

1.4 Arkivnummer/saksnummer eller andre viktige kjennetegn for virksomheten

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

1.5 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.

Deltakerne som deltar i vurderingen, bør samlet ha bred kompetanse om behandlingen. Aktuelle deltakere/roller i en personvernkonsekvensvurdering:

- Systemansvarlig
- Personvernrådgivere
- Innkjøpsansvarlig
- Personer som skal utføre selve behandlingen av personopplysninger (ansatte)
- IT/CISO (Bør delta aktivt for å belyse tekniske sårbarheter og trusselbildet)
- Leverandør
- Personvernombud
- Representanter for den registrerte

1.6 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 ved 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.

1.7 Versjonshistorikk

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

I tillegg til planlagt, periodisk gjennomgang (se punkt 5.3), 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, for eksempel ytterligere behandlingsaktiviteter eller endre en pågående behandlingsaktivitet
- Endring i teknisk løsning
- Ved store endringer i system/behandling bør det vurderes om hele personvernkonsekvensvurderingen bør gjøres på nytt.
- Der personvernkonsekvensvurderingen er basert på en vurdering som er delt fra en annen virksomhet, som omhandler samme/tilsvarende behandling (gjenbruk av personvernkonsekvensvurdering).

1.8 Oversikt over 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.

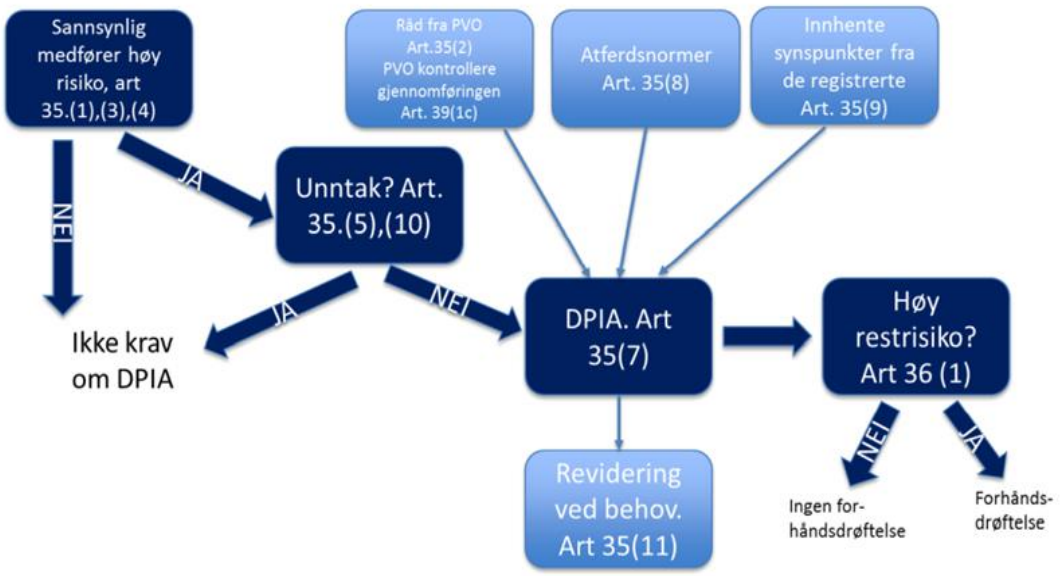
Veiledning til del B: Behovsvurdering

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.

2.1 Indikasjoner på at personvernkonsekvensvurdering må gjennomføres

Her skal virksomheten identifisere behov for om en personvernkonsekvensvurdering må gjennomføres.

Følgende figur illustrerer behandlinger som medfører høy risiko for de registrertes rettigheter og friheter.[18] På nåværende punkt i malen/veilederen så er virksomheten i boksen «Sannsynlig medfører høy risiko» i dette skjemaet.



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).

[18] https://ec.europa.eu/newsroom/article29/items/611236
https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/edpbartikkel29gruppen/Veileder-i-vurdering-av-personvernkonsekvenser-wp-248-norsk.pdf

2.1.1 Virksomheten har allerede identifisert at behandlingen fører til/ fører ikke til høy risiko

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 til 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 vil 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 nedlastingen 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.

2.1.2 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.[19,20]

Virksomheten velger et eller flere elementer 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.

[19] https://ec.europa.eu/newsroom/article29/items/59485/en
[20] 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 likevel være nyttig å gjennomgå kravene fra WP29-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).

2.1.3 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.

2.1.4 Krav i artikkel 29-gruppens veileder er oppfylt

Her skal virksomheten vurdere om krav i artikkel 29-gruppens veileder er oppfylt. WP 29 har det lagt til grunn ni relevante kriterier for å avgjøre hvorvidt en behandling vil føre til høy risiko eller ikke.[21]

Det er anbefalt å gjennomføre en personvernkonsekvensvurdering dersom to eller flere kriterier er oppfylt, men dette er ikke absolutt. Virksomheten må gjøre en konkret vurdering.

For eksempel kan en virksomhet behandle store mengder opplysninger om sårbare grupper, men det er lite sensitive data eller pseudonymiserte data[22], som gjør at risikoen anses som lav.

Kravet til en god begrunnelse for ikke å gjøre en personvernkonsekvensvurdering blir høyere dess flere kriterier som er oppfylt.

De ni kriteriene er:

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

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

- 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». [23]
- 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.

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

Det kan forekomme tilfeller der risikoen kan vurderes som høy, selv om behandlingen ikke er særskilt nevnt i Datatilsynets liste eller i WP29 gruppens veileder. Virksomheten må dokumentere vurderingen og beskrive hvilke momenter den har lagt vekt på.

2.1.6 Virksomheten har tidligere hatt konsesjon[24] fra Datatilsynet eller godkjenning fra REK som er datert før juli 2018.

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.

[23] Ref. fortalepunkt 71 og 91.
[24] https://www.datatilsynet.no/regelverk-og-verktoy/konsesjon-og-melding/

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 i punkt 2.7.

2.1.7 Virksomheten har tidligere utført en personvernkonsekvensvurdering, og ser et behov for å oppdatere med en ny personvernkonsekvensvurdering.

Virksomheten bør si noe om hvorfor det er nødvendig å oppdatere med ny personvernkonsekvensvurdering, og hva de konkrete endringene består i.

2.2 Har personvernombudet uttalt seg i vurderingen av behovet for å gjennomføre en personvernkonsekvensvurdering?

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

Personvernombudets anbefaling, samt dato for anbefaling oppgis her.

Dersom vurderingen er et eget dokument, legg til i lista over vedlegg i punkt 2.7.

2.3 Virksomheten har besluttet at

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

2.4 Sett inn begrunnelsen for hvorfor virksomheten har kommet til at det skal/ikke skal gjennomføres en personvernkonsekvensvurdering

Her skal virksomheten dokumentere sin beslutning.

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 WP29-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.

Veiledning til del 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.

3.1 Beskriv det overordnede formålet med den planlagte behandlingen av personopplysninger

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[25] og Normens faktaark Formål og behandlingsgrunnlag[26].

3.2 Hvem er de registrerte?

Her skal virksomheten oppgi hvilke kategorier av registrerte som det skal behandles opplysninger om. Dersom alternativene i malen ikke er tilstrekkelige, kryss av for «andre» og beskriv.

3.3 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 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.

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».

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

3.4 Beskriv relasjonen mellom dataansvarlig/representant for dataansvarlig og de registrerte

Her skal virksomheten beskrive hvilken relasjon den registrerte har til dataansvarlig, f.eks. lege og pasient. 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 hvor det kan forekomme skjevheter i maktforholdet er der hvor en enkeltperson setter frem krav om en ytelse fra NAV. Vedtaket treffes av den som er dataansvarlig. Utfallet av vedtaket vil påvirke den registrertes økonomiske situasjon og det anses å være betydelige skjevheter i maktforholdet her.

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

3.5 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?

Se mer om hva som anses som stor skala og hvilke relevante momenter som skal legges til grunn i punkt 2.1

3.6 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.

Dersom vurderingen gjelder flere behandlingsaktiviteter, så må virksomheten kopiere og lime inn skjemaet under så mange ganger det er nødvendig for å få beskrevet alle behandlingsaktivitetene. Dersom virksomheten har definert bestemte kategorier/typer behandlingsaktiviteter, tilpasses malen ved å kopiere tabellen i samsvar med det.

Virksomheten kan velge å kategorisere eller gruppere typer aktivitet. Har virksomheten definert bestemte kategorier/typer behandlingsaktiviteter, tilpasses malen ved å kopiere tabellen i samsvar med det.

Punkt i malen	Veiledning til utfylling
Behandlingsaktivitet:	Se kapittel om begrep.
Formål:	Formålet med behandlingen angis. Det bør også vurderes om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålet/formålene. Dersom virksomheten kommer frem til at det er avvik fra hva som er det opprinnelige formålet og den behandlingsaktiviteten som planlegges, 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. Helseopplysninger er særlig kategori av opplysninger.
Lagringstid:	Hvor lenge lagres opplysningene?

3.7 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 opphører, 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 punkt 3.9 om leverandører.

På dette punktet kan dialog med leverandører og databehandlere være nyttig. Legg gjerne med flytskjema ol i listen over vedlegg, punkt 2.7.

3.8 Utdyp forhold som ikke fremgår tydelig av beskrivelsen av dataflyt

Bruk av ny 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.

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, 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.

3.9 Beskriv bruk av leverandører (inkludert databehandlere) og relasjonen til disse

Her skal virksomheten gi en oversikt over alle leverandører den benytter seg av, inkludert underleverandører/ underdatabehandlere. Relasjonen til disse defineres i databehandleravtaler og innholdet i avtalene kan beskrives i dette punktet.

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 eksisterer utenfor EU/EØS.[27]

Legg gjerne med avtaler ol i listen over vedlegg, punkt 2.7.

3.10 Annen informasjon

I dette feltet i malen kan virksomheten beskrive eller utdype momenter ved behandlingen av personopplysninger som virksomheten mener er av betydning.

Dette kan særlig være der viktige momenter ikke kommer tydelig frem gjennom utfylling av de øvrige feltene i del C.

3.11 Hvordan vil virksomheten opptre i samsvar med de generelle personvernprinsippene?

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

[27] https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/retningslinjer-og-uttalelser-fra-personvernradet/utfyllende-veiledning-om-schrems-ii/

For mer om innholdet i de ulike rettighetene, se Datatilsynet[28] og Normens faktaark Personvernprinsippene[29]. I veilederen finnes også informasjon om eventuelle unntak fra plikten til å oppfylle rettighetene.

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 se punkt 2.7.

3.12 Hvordan har virksomheten planlagt at den skal ivareta de registrertes rettigheter?

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[30] og Normens Veileder for rettigheter ved behandling av helse- og personopplysninger[31]. 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 se punkt 2.7.

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).

[28] https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/
[29] https://www.ehelse.no/normen/faktaark/faktaaark-57-personvernprinsippene
[30] https://www.datatilsynet.no/rettigheter-og-plikter/den-registrertes-rettigheter/
31 https://www.ehelse.no/normen/veiledere/veileder-for-rettigheter-ved-behandling-av-helse-og-personopplysninger

3.13 Dersom behandlingen av personopplysninger gjelder et system/løsning, hvordan er personvern bygget inn?

Personvern som standardinnstilling er et krav i personvernregelverket. Ved å bygge inn personvernet i løsninger, systemer eller programvare som benyttes i forbindelse med en behandling av personopplysninger, kan virksomheten sørge for etterlevelse av personvernprinsipper og ivaretakelse av de registrertes rettigheter.

Her skal virksomheten beskrive hvordan innebygd personvern er en del av virksomhetens løsning.

Veiledning til del 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). Merk at denne risikovurderingen ikke handler om hvilken risiko virksomheten løper på egne vegne, men hvilke risikoer behandlingen av personopplysninger 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, 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 den samlede 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 den registrerte og hvorfor?

I punkt 4.1 og 4.2 i malen skal virksomheten beskrive hvorfor behandlingen er nødvendig. En slik nødvendighetsvurdering skal alltid gjøres, uavhengig av om behandlingen krever en personvernkonsekvensvurdering etter artikkel 35. Det er lurt å gjøre en ny vurdering av dette i forbindelse med personvernkonsekvensvurderingen (punkt 4.1 og 4.2), fordi målet er å komme frem til tiltak som kan redusere den høye risikoen virksomheten har identifisert. Implisitt i dette ligger at virksomheten på nytt vurderer om personvernprinsippene oppfylles.

4.1 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. Når den gjør en slik vurdering, 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 veiledning om hvordan virksomheten konkret kan gå frem for å gjøre dette, se Datatilsynets sjekkliste[32] for vurdering av personvernkonsekvenser (del 2. om nødvendighet og proporsjonalitet), samt Normens Faktaark om personvernprinsippene[33].

Ta utgangspunkt i det dere fylte ut i punkt 3.5 i malen. Der skal dere ha redegjort for ulike aktiviteter, tilhørende formål og tatt stilling til behandlingsgrunnlag.

4.2 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.

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?

4.3 Beskriv hvilke risikoer for de registrertes rettigheter og friheter virksomheten har identifisert

Her skal virksomheten beskrive de identifiserte risikoene. 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 vil uansett måtte sees i sammenheng, og som et minimum bør den vurderingen som ferdigstilles først oppdateres etter at den andre er ferdig, for å sikre at alle relevante risikomomenter er ivaretatt.

4.4 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. 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).

Ta utgangspunkt i risikoene under, og eventuelt andre identifiserte risikoer, og før den enkelte risiko opp i tabellen i punkt 4.3 i malen. Virksomheten må kopiere og lime inn skjemaet under så mange ganger det er nødvendig for å få beskrevet alle aktuelle risikoer for de registrertes rettigheter og friheter

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

Eksempler på mulige risikoer og konsekvenser:

- Manglende reell medbestemmelse
- Manglende reell åpenhet
- Manglende forutsigbarhet
- Svekkelse av opplysningenes integritet eller redusert/manglende konfidensialitet
- Manglende informasjon
- Ikke mulighet for innsyn
- Ikke mulighet for retting og/ eller sletting
- Ikke mulighet til å protestere

Eksempler på mulige konsekvenser som kan følge:

- Risiko for forskjellsbehandling
- Risiko for identitetstyveri eller -bedrageri
- Risiko for økonomisk tap
- Risiko for skade på omdømme for den registrerte
- Risiko for tap av fortrolighet for taushetsbelagte personopplysninger
- Risiko for uautorisert oppheving av pseudonymisering[34]
- Risiko for andre økonomiske eller sosiale ulemper
- Risiko for 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)
- Risiko for nedsatt livskvalitet (f.eks. dersom behandlingen utløser bekymring hos den registrerte)
- Risiko for krenkelse av integritet/integritetstap
- Risiko for at 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. For å lese mer om de enkelte rettighetene, se Normens Veileder for rettigheter ved behandling av helse- og personopplysninger[35].

Punkt i malen	Veiledning til utfylling
Beskriv konsekvensen for fysiske personers rettigheter eller friheter, som kan oppstå:	Ta utgangspunkt i risikoene i listen over. 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.

[34] Les mer om dette her https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/hvordan-anonymisere-personopplysninger/
[35] Mer om rettigheter i Normens veileder https://www.ehelse.no/normen/veiledere/veileder-for-rettigheter-ved-behandling-av-helse-og-personopplysninger

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 /konsekvensen 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 demper 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. Eksempel: Kan vi som virksomhet 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? 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. Forklaring: Forskjellsbehandling (se oversikt over risikoer ovenfor) følger i dette eksempelet av et brudd med personvernprinsippet om opplysningenes riktighet.
Beskriv planlagte tiltak som skal dempe risikoen ytterligere:	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:

Eksempler på utfylling

Store mengder helseopplysninger og personopplysninger av svært personlig karakter behandles			
De registrerte unntas fra retten til informasjon og kjenner da heller ikke til øvrige rettigheter de har i forbindelse med at det behandles personopplysninger om dem.			
Hvilke(n) behandlingsaktivitet(er) er konsekvensen relatert til:	Det skal innhentes opplysninger om svært mange personer fra et sentralt helseregister og det vil ikke være mulig å informere alle individuelt.		
Beskriv hvor sannsynlig det er at konsekvensen oppstår:	Svært sannsynlig, da ingen mottar individuell informasjon. Prosjekter som får utlevert personopplysninger fra registeret beskrives på registerets nettsider, men det er ikke sannsynlig at denne informasjonen vil nå alle de registrerte selv om de er informert om at de er registrert i dette registeret.		
Beskriv hvilke konsekvenser dette kan få for den registrerte:	For de som ikke blir kjent med at personopplysninger om dem behandles til dette formålet (kvalitetssikring av helsetjenesten), vil de heller ikke gjøres kjent med hvilke andre rettigheter de har i hht. Behandlingsgrunnlaget (helseregisterloven?) og rettighetene som følger av denne og personvernforordningen.		
Beskriv eksisterende tiltak som demper risikoen:	Prosjekter som får utlevert personopplysninger fra registeret beskrives på registerets nettsider, men det er ikke sannsynlig at denne informasjonen vil nå alle de registrerte selv om de er informert om at de er registrert i dette registeret.		
Beskriv virksomhetens vurdering av om risikoen er akseptabel:	Helseforetaket har jf. Pasient- og brukerrettighetsloven § 5-3 gjort en vurdering av behovet for å gi informasjon om behandlingen. Da dette ikke er et rent internt kvalitetssikringsprosjekt hvor de registrerte kan forvente at deres personopplysninger behandles og hvor den direkte nytten av kvalitetssikringsprosjektet er mer åpenbar, er det vår oppfatning at vi i denne forbindelsen bør iverksette ytterligere tiltak for å nå de registrerte, og slik oppfylle personvernprinsippet om åpenhet/transparens og sette de registrerte i stand til å benytte rettighetene sine. Ifølge Pasient- og brukerrettighetsloven § 5-3, har pasienten rett til å motsette seg overføring og tilgjengeliggjøring av journal, med mindre tungtveiende grunner taler for at overføringen bør skje.		
Beskriv planlagte tiltak som skal dempe risikoen ytterligere:	Pasientgruppen har felles kjennetegn i form av to kreftrelaterte diagnoser. Det vil etter vår oppfatning kunne redusere risikoen for at informasjonen ikke når de fleste, dersom vi formidler informasjon via pasientforeningen/kreftforeningen.		
Ansvarlig for tiltak:	Rolle…..	Frist:…..	

Behandling av personopplysninger om sårbar gruppe/sårbare registrerte. Ujevnt maktforhold mellom pasient og dataansvarlig. Er det mulig å benytte samtykke som lovlig behandlingsgrunnlag, gitt det skjeve maktforholdet?			
Hvilke(n) behandlingsaktivitet(er) er konsekvensen relatert til:	Pasientsvarskjema relatert til opplevde plager etter gjennomført undersøkelse av spiserøret. (Kvalitetssikring). Pasientsvarskjemaet er basert på samtykke. Øvrig behandling har behandlingsgrunnlag i helselovgivningen.		
Beskriv hvor sannsynlig det er at konsekvensen oppstår:	Det er sannsynlig at pasienter ikke opplever at de har en reell anledning til å si nei til å besvare skjemaet. De har ikke selv noen direkte nytte av at behandlingen skjer, men kan oppleve at må besvare for å sikre upåvirket videre oppfølging i behandlingsforløpet.		
Beskriv hvilke konsekvenser dette kan få for den registrerte:	Den registrerte unnlater å benytte seg av rettighetene sine og slik sett ivareta sitt eget personvern.		
Beskriv eksisterende tiltak som demper risikoen:	Det understrekes at det er frivillig å besvare skjemaet.		
Beskriv virksomhetens vurdering av om risikoen er akseptabel:	Akseptabel, da skjemaet ikke skal inneholde andre opplysninger enn behandlende lege selv vil motta muntlig i sin oppfølging. Vi velger likevel å iverksette ytterligere tiltak som er relativt enkle å iverksette.		
Beskriv planlagte tiltak som skal dempe risikoen ytterligere:	Informasjon gis og samtykke innhentes av en annen enn behandlende lege.		
Ansvarlig for tiltak:		Frist:	

4.5 Beskriv/konkretiser hvilke risikomomenter som er vektlagt i risikovurderingen

Her skal virksomheten oppsummere det som samlet fremgår av tabellene hvor risikoene er beskrevet. En slik oppsummerende beskrivelse av identifiserte risikoer og fokusområder vil gjøre det lettere for beslutningstakere å ta stilling til om personvernkonsekvensvurderingen er dekkende.

Veiledning til del E: Innspill og ledelsens beslutning

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

5.1 Hvilke innspill har virksomheten fått fra registrerte (eventuelt representanter for de registrerte) og andre interessenter?[36]

Her skal virksomheten beskrive om den har innhentet innspill fra den registrerte eller representanter for den registrerte og hvilke innspill som er kommet.

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 i punkt 1.4.

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.

Det kan være hensiktsmessig å 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 senke en risiko har blitt innført, eller at en rutine for å oppfylle rettigheter har blitt endret.

5.2 Hvilke anbefalinger har personvernombudet gitt?

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 gjennomføringen av personvernkonsekvensvurderingen. Dette innebærer at ombudet i etterkant av vurderingen skal kontrollere at den dekker minimumskravene i

[36] 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.

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 i punkt 2.7.

5.3 Hva er 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. Basert på restrisikoen skal ledelsen beslutte om de vil akseptere risikoen og gjennomføre behandlingen, eller om restrisikoen er for høy. Dersom ledelsen ikke aksepterer risikoen, men allikevel ønsker å gjennomføre behandlingen, må det gjennomføres forhåndsdrøfting med Datatilsynet.[37]

Ledelsen skal dokumentere begrunnelsen skriftlig, og signeres av leder eller den som har myndighet til å signere.

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 dokumenteres i malens punkt. 1.6.

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

Direktoratet for e-helse

Besøksadresse
Verkstedveien 1
0277 Oslo

Postadresse
Postboks 6737
St. Olavs plass