Personvernkonsekvensvurdering

(DPIA - Data Protection Impact Assessment)

Kort beskrivelse av gjennomføring av DPIA ved bruk av dette verktøyet:

Benyttede arkfaner:

"Initialvurdering" Innledende grunnleggende informasjon, deltakere, initielle spørsmål som avdekker om behov for full DPIA eller ikke.

Dersom konklusjon av initialvurdering er full DPIA:

"Systematisk beskrivelse" Grundig gjennomgang av behandlingen og dennes omfang.

"Nødvendighet og proporsjonalitet" Påvise at forordningen etterleves og at rettigheter og friheter ivaretas.

"Risikovurdering" Vurdere uønskede hendelser og risikoen og årsak for disse, og deretter foreslå/anbefale tiltak for å mitigere risikoen.

"Rapport" Rapport "genereres" fra de tidligere fanene. Må fylles ut videre fra "(6) Vurdering og synspunkter til behandlingen og dens risikoer (restrisiko):", deltakernes vurdering og felles konklusjon. Til sist skal behandlingsansvarlig validere, konkludere og til slutt signere.

Datatilsynet - DPIA

"Skisse Lag en skisse over løsningen og dataflyten slik at man enklere får en god forståelse av hvordan personopplysningene flyter gjennom hele behandlingen.

"Risikotabell" Basert på Bærum kommunes forankrede risikoappetitt, kan benyttes som hjelp til utfylling av sannsynlighet og konsekvens (som gir risikoverdien).

"Endringslogg" Før opp endringer utført i dokumentet, møter, møtedeltakere. Oppføringer av vedlegg og aktuelle lenker kan også legges inn her som ytterligere dokumentasjon.

"Skjules" Data/input til nedtrekksmenyer etc ligger her (noe ustrukturert og kan hende må tilpasses noe). Denne fanen bør skjules når verktøy tas i bruk.

Datatilsynet:
"Vurdering av personvernkonsekvenser (DPIA)
En vurdering av personvernkonsekvenser (Data Protection Impact Assessment - DPIA) skal sikre at personvernet til de som er registrert i løsningen ivaretas. Dette er en plikt etter det nye personvernregelverket. Artikkel 35 definerer når det er påkrevd å gjøre en DPIA, hva den skal inneholde og hvem som skal gjennomføre den."

Personopplysningsloven Artikkel 35

Hvordan gjennomføre en DPIA?

Det finnes ulike metoder for å gjennomføre en vurdering av personvernkonsekvenser (DPIA), men de har noen felles kriterier.
I forordningen fastsettes noen minimumskriterier for hva en vurdering av personvernkonsekvenser skal inneholde (artikkel 35 nr. 7):

a) En systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen.

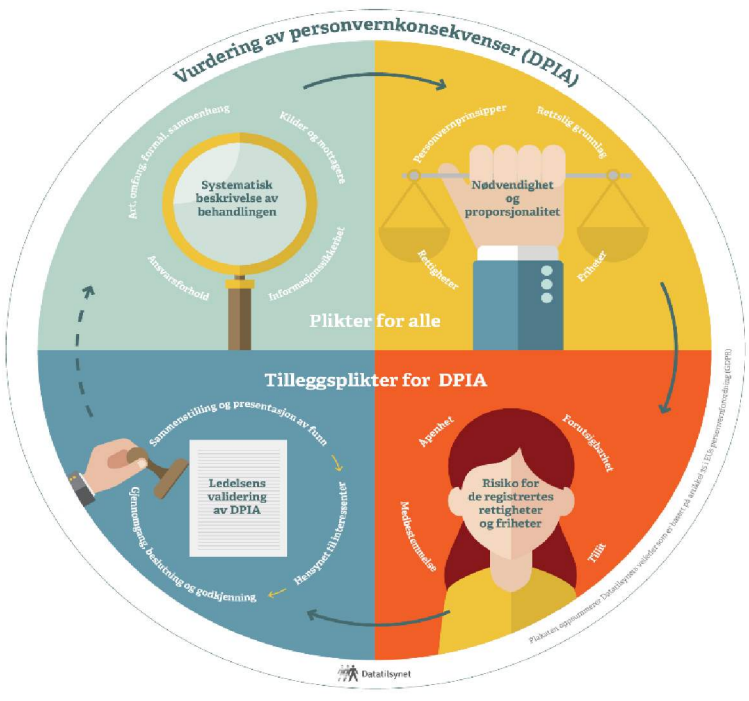
Arbeidsgruppen 29 (WP29) - Veileder

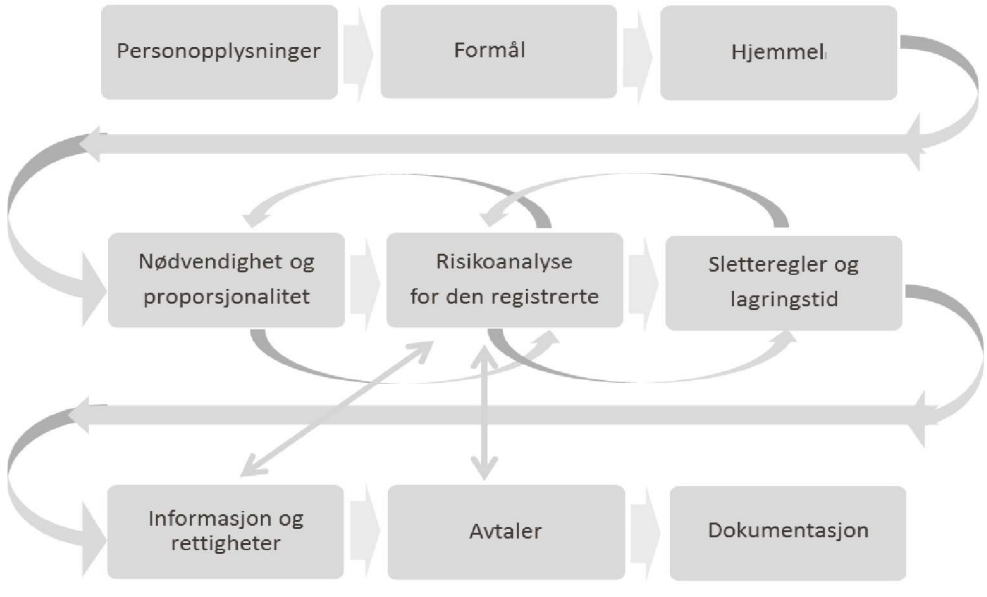
b) En vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene.

c) En vurdering av risikoene for de registrertes rettigheter og friheter

d) De planlagte tiltakene for å håndtere risikoene og for å påvise at forordningen overholdes.
I tillegg er ansvarlighet et viktig personvernprinsipp, så til slutt må man bedømme og evaluere, og eventuelt godkjenne. I denne fasen har ledelsen eller styret den viktigste rollen. Arbeidet skal sammenstilles og funn presenteres for ledelsen.

Figur 1 (under) oppsummerer og illustrerer den alminnelige, gjentakende prosessen ved gjennomføring av en vurdering av personvernkonsekvenser:





Figur 2 - Oversikt over stegvis prosess for personvernskonsekvensvurderingen

Personvernkonsekvensvurdering
(DPIA - Data Protection Impact Assessment)

Hensikt med DPIA	Det er obligatorisk å utføre en personvernkonsekvensvurdering (DPIA) dersom det er sannsynlig at en type behandling av personopplysninger kan medføre en høy risiko for fysiske personers personvern, deres rettigheter og friheter (personvernforordningen, artikkel 35). Personvernkonsekvensvurderingen skal utføres *før* behandlingen starter og skal alltid være vurdert av personvernombudet.

(1) Innledende informasjon

Organisasjonsenhet/ sektor:	Helse- og omsorg
Kommunalsjef/ behandlingsansvarlig:	**Oddvin A. Neset**
Navn på behandling som vurderes: *(Tjeneste, system, anskaffelse, prosess etc)*	Pleie- og Omsorgssystem - Visma PROFIL
Type behandling/ behandlingsaktiviteter: (Overordnet beskrivelse og omfang av behandling av personopplysninger)	Elektronisk journal system for Helse/Pleie og omsorg.
Formål (Mål, hensikt, gevinst ved behandlingen (Art. 5b))	Sikre forsvarleg helsehjelp. Sikre forsvarleg journalføring.
Rettslig grunnlag/ behandlingsgrunnlag (Det må finnes et lovlig grunnlag (Art. 5a, 6.1) (*Ved flere rettslige grunnlag, benytt også kommentarfelt*))	Oppfylle rettslig forpliktelse (lov) (art. 6.1 c)
Hjemmel (Ved lovpålagt tjeneste, allmenn interesse, offentlig myndighet (Art. 6.3))	Journalforskrifta. Pasient- og brukerrettighetsloven. Helsepersonellova. Offentlighetslova. Lov om kommunale helse og omsorgsteneste. Normen.
Kommentarer til innledende informasjon:	

Deltakere - Viktig at alle interessenter er representert ved full DPIA	
Behandlingsansvarlig eller delegert ansvarleg/representant:	Beate I. Matre, Elin Eikemo. Ernestas Janciauskas, Frida Eide, Monica Rongved
Personvernombud:	Bård Harry Bolstad Eikefet
Representant(er) for den/de registrerte: Begrunn dersom det ikke er relevant å innhente deres synspunkter (Art. 35.9)	Asbjørn Bjørneklett
Andre: (Eks. prosjektleder, jurist, IT-sikkerhet, IT-drift, databehandler)	Visma
Kommentarer til deltakere:	

DPIA - Initiell vurdering **Vurdering av behandlingsaktiviteter og om full analyse kreves**	**Ja/Nei** (Velg fra nedtrekksmeny)
(1) Omfatter behandlingen særlige kategorier av personopplysninger, eller personopplysninger av meget personlig karakter? Rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske og biometriske opplysninger, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold, eller seksuelle orientering (Art. 9), straffedommer og lovovertredelser (Art. 10)	Ja
(2) Innebærer behandlingen prediksjon av atferd, profilering av, rangering av, evaluering eller poengsetting av individer?	Ja
(3) Innebærer behandlingen automatiserte beslutninger som får effekt for den registrertes rettigheter? Gjennomføres det en automatisert beslutningsprosess, enten helt eller delvis, som har rettslig eller tilsvarende betydelig virkning for den fysiske personen?	Nei
(4) Innebærer behandlingen systematisk overvåking av den registrerte? Kontinuerlig overvåkning av den registrerte, eller overvåkning av offentlig rom, slik at den registrerte ikke nødvendigvis er klar over at han/hun overvåkes, eller at det kan være vanskelig for den registrerte å unngå overvåkingen (eksempelvis videoovervåking av offentlig tilgjengelig område, bruk av lokasjonsdata, kontroll av ansatte (effektivitet, ferdigheter, kunnskap, mental helse)). **Merk at: Systematisk overvåking/monitorering av ansatte medfører alltid full DPIA**	Nei
(5) Gjennomføres det behandling i stor skala? Høyt antall registrerte eller høy prosentdel av innbyggere, stor mengde data, mange ulike typer data, dekker stort geografisk område, eller foregår over lengre tid, herunder permanent Høyt antall registrerte eller høy prosentdel av registrerte, stor mengde personopplysninger, mange ulike typer personopplysninger, dekker stort geografisk område, eller foregår over lengre tid, herunder permanent.	Ja
(6) Brukes personopplysningene for å avdekke ukjente sider eller for å gjenkjenne mønstre ved den registrerte gjennom matching/sammenstilling, og videre benytte dette til hensikter som det var vanskelig for den registrerte å forestille seg? Datasett fra to eller flere behandlingsoperasjoner, gjennomført med forskjellige formål og/eller av ulike behandlingsansvarlige, slås sammen og kan nyttes til et nytt formål som det var vanskelig for den registrerte å forestille seg.	Nei
(7) Omfatter behandlingen personopplysninger om sårbare registrerte? Sårbare individer er i en svak maktposisjon i forhold til den som behandler data, og har derfor begrenset evne til å motsette seg. Sårbare registrerte kan omfatte barn, psykisk syke, pasienter, rusavhengige, asylsøkere, eldre og arbeidstakere.	Ja
(8) Omfatter behandlingen innovativ bruk av personopplysninger eller bruk av teknologiske eller organisatoriske løsninger, hvor tilknyttet risiko enda ikke er kjent? Eksempelvis nye app'er, velferdsteknologi, "tingenes internett" (IoT) eller kunstig intelligens (AI).	Nei
(9) Hindrer behandlingen den registrerte i å utøve en rettighet, en tjeneste, eller en kontrakt? Når behandlingen har det formål å begrense hvem som får tilgang til noe, f.eks. en beslutningsprosess hvor man avgjør hvem som får tilskudd eller ikke. Punktet omfatter også overvåkning av offentlig rom som man må passere for å komme et sted.	Nei
(10) Er personopplysningene samlet inn via en tredjepart (ekstern leverandør)? For eksempel innsamling og sammenstilling av personopplysninger fra tredjeparter for å avgjøre om den registrerte skal få tilbud om, fortsette å motta, eller nektes et produkt, en tjeneste eller et tilbud.	Ja
Kommentarer til vurderingene:	Punkt 10: Mottar informasjon frå eksempelvis spesialisthelsetenester, og privat omsorgtenester, med meir.

Konklusjon initiell vurdering (Velg fra nedtrekksmeny):	**Full DPIA**
Det er to "Ja" eller flere, det vurderes derfor at det er sannsynlig at behandlingen vil innbære en høy risiko for fysiske personers personvern, deres rettigheter og friheter - full DPIA skal gjennomføres	**Ja**

(2) Systematisk beskrivelse av behandlingen

2.1 Formål

Behandlingens formål (preutfylles fra fanen Initialvurdering)

Sikre forsvarleg helsehjelp.
Sikre forsvarleg journalføring.

Vil behandlingen av personopplysninger ha som mål å ta beslutninger som får betydning for den registrerte?	Ja	**Nedtrekksmeny**
Innebærer behandlingen prediksjon av atferd, profilering av, rangering av, evaluering eller poengsetting av individer? (preutfylles fra fanen Initialvurdering)	***Ja***	
Brukes personopplysningene for å avdekke ukjente sider eller for å gjenkjenne mønstre ved den registrerte? Gjelder også sammenstilling av opplysninger og bruk til andre formål enn oppgitt/infomert (preutfylles fra fanen Initialvurdering)	***Nei***	
Brukes personopplysningene for å avdekke ukjente sider eller for å gjenkjenne mønstre ved den registrerte gjennom matching/sammenstilling, og videre benytte dette til hensikter som det var vanskelig for den registrerte å forestille seg?	Nei	**Nedtrekksmeny**
Vil personopplysningene viderebehandles til nye eller andre formål?	Ja	

Personopplysingar vil bli anonymisert og pseudonymisert ved innsending til KPR for statistikk.

Vurdering av om formålet er godt nok beskrevet: Ok — Nedtrekksmeny **Mangel/risiko**

2.2 Behandlingsgrunnlag

Behandlingsgrunnlag (preutfylles fra fanen Initialvurdering)

Oppfylle rettslig forpliktelse (lov) (art. 6.1 c)

Beskriv/begrunn behandlingsgrunnlaget

Sikre opplysingar som er relevante og nødvendige for behandling av pasienten bli nedteikna og kan finnast igjen.

Hjemmel (ved lovpålagt tjeneste) (preutfylles fra fanen Initialvurdering)

Journalforskrifta.
Pasient- og brukerrettighetsloven.
Helsepersonellova.
Offentlighetslova.
Lov om kommunale helse og omsorgsteneste.
Normen.

Evt. kommentar til 2.2 Behandlingsgrunnlag:

Vurdering av om behandlingsgrunnlaget er godt nok beskrevet: Ok — Nedtrekksmeny **Mangel/risiko**

2.3 Behandlingens art

Hvem samles det inn personopplysninger om (kategorier registrerte, eksempelvis ansatte, elever, barn, innbyggere, pasienter, kryss av for aktuelle)?

Kategorier av registrerte	Innhentet (Velg "X")	Kommentar
Innbyggere	X	*Kun som tjenestemottakere i kommunen*
Ansatte	X	
Barn/ungdom	X	*Kun dersom de er brukere i Profil, eller som pårørande*
Foreldre/foresatte	X	*Evt. som pårørende*
Elever	X	*Kun dersom de er brukere i Profil*
Eldre	X	
Pasienter	X	
Asylsøkere	X	*Kun dersom de er brukere i Profil*
Politikere	Nei	
Beredskapshjem/fosterforeldre	X	*Kan forekomme i Profil*
Slektninger/nettverk/venner	X	*Kun som pårørende*
Institusjoner/myndighetspersoner	Nei	
(Legg til flere ved behov)		

Hvordan samles personopplysningene inn (samles opplysningene inn fra den registrerte selv og/eller andre kilder)?

Personregisteret for å registrere ein pasient.
Pårørande og helseopplysinger blir henta frå pasienten.
Får informasjon frå alle partar som samhandlar rundt pasienten (spesialist helseteneste, etc.)

Hvor behandles og lagres/oppbevares personopplysningene (eks.: lokalt, i sky)?

Lokal installasjon i kommunene

Hvordan lagres personopplysningene (format, eks. database, tekstdokument, regneark, papir)?

SQL Database

Geografisk omfang av behandling (lokalt i kommunen, eksternt hos leverandør, i Norge, EU/EØS, 3. land)?

Lokalt i kommunen

Hvem har tilgang til personopplysningene (eks. saksbehandler, IT-operatør, leverandør etc)?

Profil er installert lokalt og ingen fra leverandøren har behov for personopplysninger.
Dei med gyldig grunn har tilgang til informasjon (yte helsehjelp, saksbehandling).

Brukes det ny teknologi eller eksisterende teknologi hvor personvernkonsekvenser ikke har blitt vurdert? (preutfylles fra fanen Initialvurdering)	***Nei***

Evt. kommentar til 2.3 Behandlingens art:

Vurdering av om behandlingens art er godt nok beskrevet: Ok — Nedtrekksmeny **Mangel/risiko**

2.4 Behandlingens omfang

Hvilke typer av alminnelige personopplysninger behandles (kryss av for aktuelle)?

Type personopplysning	Innhentet (Velg "X")	Årsak innhenting (Benyttes ved behov)	Hentet fra (Benyttes ved behov)
Fornavn	X		
Etternavn	X		
Adresse	X		
Telefonnummer	X		
Epostadresse	x		
Personnummer	X		
Fødselsnummer	X		
(Legg til alle innhentede personoppl.)	X	*Informasjon om klient som navn, fødsels- og personnummer, adresse, telefon, sivilstatus, fødested, nasjonalitet, språk, nåværende og tidligere yrke, umyndiggjort, kontaktpersoner (nærmeste pårørende, relasjoner, fastlege etc), organisatorisk tilhørighet etc Post- og saksbehandling, arkiv, SvarUt etc. Medisinsk informasjon som tjenster, diagnoser, medisiner, cave, allergier, tiltaksplaner, prøvesvar, målinger, IPLOS, Bruk av tvang, tekniske hjelpemidler etc. Dagsenteropphold, Institusjonsopphold, Boligtilknytning etc Elektronisk kommunikasjon mellom Pleie- og Omsorg og fastlege, sykehus, helsenorge. Etc. Logg over all elektronisk kommunikasjon etc. Innbyggerdialog mellom Pleie- og Omsorg og klient/pårørende Egenbetaling, fakturagrunnlag, vederlagsberegning (inntekter og fradrag), inntektsopplysninger, meldinger til/fra NAV, pasientregnskap etc*	

Omfatter behandlingen særlige kategorier av personopplysninger, eller personopplysninger av svært personlig karakter? **Rase, eller etnisk opphav, politiske meninger, religiøs eller filosofisk oppfatning, fagforeningsmedlemskap, genetiske data, biometriske data som kan identifisere en enkeltperson, helsedata, beskrivelse av kjønnsliv, eller seksuell orientering** (preutfylles fra fanen Initialvurdering)	***Ja***

Hvilke særlige kategorier av personopplysninger behandles (kryss av for aktuelle)?

Type personopplysning	Innhentet (Velg "X")	Årsak innhenting (Benyttes ved behov)	Hentet fra (Benyttes ved behov)
Rasemessig eller etnisk opprinnelse	X	*Samler inn om person er norsk statsborgar. Potensielt i forhold til statistikk*	*Pasienten sjølv*
Politisk oppfatning	Nei		
Religion	X	*Samler inn ved relevanse for pasienten sine behov.*	*Pasienten sjølv*
Filosofisk overbevisning	Nei		
Fagforeningsmedlemskap	Nei		
Genetiske opplysninger	Nei		
Biometriske opplysninger	Nei		
Helseopplysninger	X	*For å yte helsehjelp*	*Registreringer, Elektroniske*
Seksuelle forhold	Nei		
Seksuell legning	Nei		
Straffedommer	Nei		
Lovovertredelser	Nei		
Umyndiggjort	X	*For å yte helsehjelp. For å vite kven ein skal ta kontakt med (Verge). Verge skal også vere invlovert i behandlinga.*	*Verge sender eit skriv frå statsforvaltar om at denne er blitt verge.*
Fritekstfelt hvor det er risiko for at kan inneholde særlige kategorier av personopplysninger (ustrukturert)	X	*Helseopplysninger behandles i Profil, med det formål å gi pasienter/brukere et forsvarlig og tilfredsstillende helsetilbud som imøtekommer den enkeltes behov, og overholder øvrig lovverk. Systemet legger ikke opp til registrering av andre*	

Antall registrerte involvert?

Omlag 770 (brukere, i snitt 2 pårørende, tilsette, leger)

Antall typer/volum av personopplysninger, detaljeringsgrad?

Henviser til punkt 2.3 og 2.4.

Frekvensen av behandlingen/systematisk behandling (innhentes en gang, flere ganger, kontinuerlig)?

Kontinuerlig som grunnlag for å yte helsehjelp

Lagringstiden for personopplysningene (tidsavgrenset, til evig tid, lovpålagt, formål oppnådd)?

Lovpålagt.

Gjennomføres det behandling i stor skala? Høyt antall registrerte eller høy prosentdel av innbyggere, stor mengde data, mange ulike typer data, dekker stort geografisk område, eller foregår over lengre tid, herunder permanent (preutfylles fra fanen Initialvurdering)	***Ja***	
Er skisse som viser flyten av personopplysninger gjennom behandlingens alle faser opprettet? Lagre flytskjemaet som: "ÅÅÅÅ-MM-DD DPIA for behandlingsnavn - Vedlegg A" eller kopier skissen til arkfanen "Skisse" i dette dokumentet.	Ja	**Nedtrekksmeny**

Evt. kommentarer til skisse: Grei beskrivelse av informasjonsflyten.

Evt. kommentar til 2.4 Behandlingens omfang:

Vurdering av om behandlingens omfang er godt nok beskrevet: Ok — Nedtrekksmeny **Mangel/risiko**

2.5 Konteksten behandlingen utføres i

Kan den registrerte oppfatte behandlingen som uforutsigbar? (Viktig at den registrerte vurderer!) **Beskriv hvordan behandlingen vil oppfattes fra den registrertes synsvinkel.**	Ja	**Nedtrekksmeny**

Kommentar: Kan vere at enkelte føler ein missmatch mellom kva som er skriven om dei, og kva dei sjølv føler om sin helsetilstand/situasjon.

Vil den registrerte ha en *særskilt* forventning om at personopplysningene er nødvendige og korrekte? (Viktig at den registrerte vurderer!)	Ja	**Nedtrekksmeny**

Kommentar: Pasient bør kunne stole på at opplysingane som ligg i journal om seg skal vere korrekte og naudsynte.

Omfatter behandlingen personopplysninger om sårbare registrerte? **Sårbare individer er i en svak maktposisjon i forhold til den som behandler data, og har derfor begrenset evne til å motsette seg. Eksempler kan være; barn, psykisk syke, pasienter, rusavhengige, asylsøkere, eldre og arbeidstakere** (preutfylles fra fanen Initialvurdering)	***Ja***

Evt. kommentarer:

Omfatter behandlingen innovativ bruk av teknologi eller organisatoriske verktøy, hvor tilknyttet risiko enda ikke er kjent? **Eksempelvis nye app'er, velferdsteknologi eller kunstig intelligens (AI)** (preutfylles fra fanen Initialvurdering)	***Nei***

Evt. kommentarer:

Matches eller sammenstilles flere datasett? **Datasett som tidligere ble behandlet av to eller flere aktører, eller med to eller flere hensikter, slås sammen og kan nyttes til hensikter som det var vanskelig for den registrerte å forestille seg når samtykke ble innhentet** (preutfylles fra fanen Initialvurdering)	***Nei***

Evt. kommentarer:

Evt. kommentar til 2.5 Behandlingens kontekst:

Vurdering av om behandlingens kontekst er godt nok beskrevet:

Godt nok beskrevet — Ok — Nedtrekksmeny **Mangel/risiko**

2.6 Innebygd personvern

Er innebygd personvern hensyntatt ved utviklingen av løsningen? (tilgangsstyring, dataminimering, sletting ivaretatt, nedtrekksmenyer heller enn fritekstfelter, "Privacy by design", art. 25)	Ja	
Er personverninnstillinger som standard på? (Ikke flere felter for personopplysninger enn nødvendig samles inn eller vises, opplysninger slettes når formål oppnådd, det finnes et lovlig formål for innsamling, muligheter for innsyn i egne opplysninger, "Privacy by default", art. 25)	Ja	**Nedtrekksmeny**
Er behandlingen av personopplysninger tilstrekkelig godt informert? (F.eks. gjennom en personvernerklæring)	Ja	

Evt. kommentarer: Informasjon i søknad om innsamling. Forvaltningskontor kan utlevere informasjonskriv om IPLOS til KPR. Legge ved eit vedlegg i vedtak om kva som blir gjort med pasientopplysingar. Informere muntlig.

Hvordan ivaretar informasjonssystemet/løsningen som benyttes til behandlingen av kravet til innebygd personvern og personvern som standardinnstilling? (Se link i fanen Endringslogg)

Visma jobber aktivt med å sikre innebygd personvern i utviklingen av nye løsninger og funksjonaliteter (privacy by design and default). Viktige momenter i dette arbeidet er å kartlegge hva formålet med løsningen/funksjonaliteten skal være, og hvilke data som er nødvendig for å oppnå formålet. Å sikre god oversikt over dataflyt internt og eksternt i løsningen, og oversikt over eventuelle tredjeparter, er et annet viktig moment. Videre opererer våre utviklere med en konkret sjekkliste som bidrar til å sikre at personvern blir en integrert del av utviklingsarbeidet. Gjennom testing, tilbakemeldinger fra kunder og jevnlige oppdateringer, jobber vi kontinuerlig for å eliminere brukerfeil og misforståelser. Vismas juridiske team bistår med å kontrollere at nye løsninger og funksjonalitet er GDPR-compliant.

Vanlige tiltak for å sikre personvern i Vismas tjenester er:
- Jevnlig testing og oppfølging av brukerfeil
- Jevnlige oppdateringer
- Tilgangsstyring gjennom rolletildeling
- Vannmerking av fritekstfelter

Vurdering av om innebygd personvern for behandlingen er godt nok beskrevet: Ok — Nedtrekksmeny **Mangel/risiko**

2.7 Bruk av databehandler

Benyttes databehandler i forbindelse med behandlingen?	Ja	**Nedtrekksmeny**
Er databehandleravtale etablert?	Ja	

Hvilke garantier gir databehandleren for at egnede tekniske og organisatoriske tiltak som sikrer at behandlingen er i samsvar med forordningen vil gjennomføres?

Profil er lokalt installert, og kommunen er både databehandler og dataansvarlig.
Er også DBA med Visma. Samt mellom kommunane og IKTNH.

Evt. kommentar til 2.7 Bruk av databehandler:

Vurdering av om bruk av databehandler er godt nok beskrevet: Ok — Nedtrekksmeny **Mangel/risiko**

2.8 Tekniske og organisatoriske sikkerhetstiltak

Er risiko- og sårbarhetsanalyse (RoS) gjennomført?	Ja	**Nedtrekksmeny**

Evt. kommentarer:

Hvilke tekniske og organisatoriske sikkerhetstiltak er implementert for å ivareta personopplysningssikkerheten?

Visma sin kommentar: "Ved bruk av Vismas support-kanaler er det normalt ikke behov for å dele flere personopplysninger enn navn og e-post på personen som sender inn saken til support. Når du som kunde henvender deg til Visma i forbindelse med support, feilretting eller behov for annen assistanse, kan ikke informasjonen (tekst, skjermbilde, vedlagte dokumenter osv.), inneholde ytterligere personopplysninger. Slike personopplysninger kan fjernes fra henvendelsen ved å streke over informasjon i skjermbilder, referere til ansattnummer i stedet for navn eller lignende.

Informasjon som sendes til Visma fra kunde behandles i våre systemer. Over tid er det umulig å garantere at vedlagte personopplysninger ikke er tilgjengelige for andre enn de som har håndtert saken. Den beste måten å forhindre personopplysninger på avveie i dette tilfellet, er å ikke sende personopplysninger i utgangspunktet.

Dersom en kunde ved en feil eller forglemmelse sender personopplysninger til Visma vil våre ansatte følge rutinen nedenfor:
1) Visma kontakter avsender og gir beskjed om at personopplysninger er kommet inn i vårt system, og beskriver Vismas rutine for å håndtere dette
2) Visma fjerner informasjonen fra systemet i den grad det er mulig. Dersom dette innebærer at en e-post eller et vedlegg må slettes, kan resultatet bli at Visma mangler nødvendig informasjon for å håndtere forespørselen.
3) Kunden kan bli bedt om å sende informasjonen på nytt, uten personopplysninger."

Sjå fane for ROS for kommunen sine tiltak.

Hvordan blir informasjonssikkerheten ivaretatt i informasjonssystemet/løsningen?

Henviser til fanen for "risikovurdering".

Hvordan blir informasjonssikkerheten av personopplysninger ivaretatt utenfor selve informasjonssystemet/løsningen (tilgang for personell ved driftsrelaterte oppgaver, tilgang på databaser, tilgang på backup etc)?

Henviser til fanen for "risikovurdering".

Er det utarbeidet rutiner for tilgangskontroll, rollebasert tilgangsstyring, autorisering (bruker/IT-personell/leverandør)?

Er utarbeida oppdatert overordna prosedyre for oppgåver, ansvar og rolle for tilgangsstyring som blir sendt Helse-og omsorgsleiar i løpet av mai -23. Vidare skal det utarbeidast spesifikk prosedyre for tilgangsstyring for Visma Profil.

Evt. kommentar til 2.8 Tekniske og organisatoriske sikkerhetstiltak:

Vurdering av om tekniske og organisatoriske sikkerhetstiltak er godt nok beskrevet:

Få oppdatert og godkjent prosedyrer når det gjeld tilgangsstyring og oppfølging på dette området. — Mangler — Nedtrekksmeny **Mangel/risiko**

(3) Nødvendighet og proporsjonalitet

3.1 Vurdering av personvernprinsippene

Personvernprinsippene

Baseres behandlingen på et tydelig rettslig grunnlag?	Ja
Er det rettslige grunnlaget gyldig og rimelig?	Ja

Hvordan vil åpenhet bli ivaretatt i behandlingen?

Pasient/brukar får informasjon gjennom vedtak, eller via søknad. Står også i vedtak at dei har rett til innsyn.

Formålsbegrensning

Er formålet klart definert? (Viktig at den registrerte vurderer!)	Ja
Samsvarer formålet forventningene til den registrerte? (Viktig at den registrerte vurderer!)	Ja
Kan formålet oppnås med anonyme eller pseudonyme alternativer?	Nei

Ikkje aktuelt eller trygt om ikkje pasient/bruker kan identifisreast.

Dataminimering

Er alle personopplysningene som samles inn nødvendige for å oppnå formålet?	Nei
Er det mulig å begrense innsamlingen av personopplysninger?	Ja
Er det mulig å redusere detaljgraden av personopplysninger?	Ja

I enkelt tilfeller vil det vere informasjon som ikkje er naudsynt som blir tatt med. Ein må heile tida jobbe for at urelevant opplysning ikkje blir tatt med.

Riktighet

Hvordan holdes personopplysningene korrekte og oppdaterte?

Dei tilsette rapporterer og utfører endringer. Pasient melder frå om flytting, endring av kontaktinformasjon og anna.

Ut fra den registrertes rettigheter, er det behov for kontradiksjon (det vil si den registrertes anledning til å imøtegå det som den behandlingsansvarlige har registrert)**?**	Ja

Ved innsyn kan dei kome med innspel til endring.

Lagringsbegrensning

Blir personopplysningene slettet når formålet er oppnådd, i så fall hvordan?	Ja

I Profil er det rettslige grunnlaget for behandling å oppfylle en rettslig forpliktelse. Sletting av data frå Profil må skje i tråd med reglene i helsepersonelloven, journalforskriften og arkivlova.

Integritet og fortrolighet

Er det det gjennomført ROS-analyse av informasjonssystemet? (preutfylles fra 2.8)	***Ja***
Brukes databehandler? (preutfylles fra 2.7)	***Ja***
Er det opprettet databehandleravtale? (preutfylles fra 2.7)	***Ja***
Er personopplysningssikkerheten tilstrekkelig ivaretatt?	Ja

Henviser til fanen for "risikovurdering".

Evt. kommentar til 3.1 Vurdering av personvernprinsippene:

Vurdering av om personvernprinsippene er godt nok beskrevet:	
	Ok

3.2 Den registrertes rettigheter og friheter

Den registrertes rettigheter

Hvordan gis informasjon om behandlingen til den registrerte?

I vedtak. Gjennom saksutredning. Står i søknad om at ein kan krevje innsyn, og at informasjon om dei blir registrert i kommunen sine datasystem.

Innsyn i egne personopplysninger

Hvordan kan den registrerte utøve retten til innsyn i egne personopplysninger?

Det er mulig å be om utskrift av journalen. Denne produseres i PDF-format og overleveres til bruker. Utførast jf prosedyre for handtering av henvendelse om utskrift av journal. Pasient kan få informasjon om kven dei skal kontakte for å få innsyn i IPLOS.

Korrigering av egne personopplysninger

Skal det være mulig for den registrerte å korrigere sine egne personopplysninger (jf formål og behandlingsgrunnlag)?	Ja

Hvordan kan i så fall den registrerte utøve denne rettigheten?

Dette skjer i hht Helsepersonellova, journalforskriften og Normen-kravene, hvor opplysninger som anses som feil e.l. kan bli rettet/slettet.

Sletting av egne personopplysninger

Skal det være mulig for den registrerte å slette sine egne personopplysninger (jf formål og behandlingsgrunnlag)?	Ja

Hvordan kan i så fall den registrerte utøve denne rettigheten?

Dette skjer i hht Helsepersonellova, journalforskriften og Normen-kravene, hvor opplysninger som anses som feil e.l. kan bli rettet/slettet.

Begrensning av behandling av personopplysninger

Hvordan kan den registrerte utøve retten til å begrense behandlingen av egne personopplysninger?

Kan svare nei til utlevering av diagnose til PLOS registeret.

Dataportabilitet

Hvordan kan den registrerte utøve retten til dataportabilitet?

Det er mulig å foreta en komplett utskrift av hele journalen for en person. Denne genereres som et pdf-dokument, og kan overleveres. På denne måten dekkes retten til dataportabilitet.

Innsigelse mot behandlinger

Hvordan kan den registrerte utøve retten til innsigelse mot behandlingen?

Kan svare nei til utlevering av diagnose til IPLOS registeret. Kan velje å avslutte eigen behandling, men kan ikkje nekte journalføring om dei skal motta behandling.

Automatiserte avgjørelser og profilering

Vil behandlingen av personopplysninger ha som mål å ta beslutninger som får betydning for den registrerte? (preutfylles fra fanen Initialvurdering)	***Nei***

Hvis behandlingen innebærer automatiserte avgjørelser og profilering, hvordan kan den registrerte reservere seg mot slik behandling?

Dette er ikke aktuelt i Profil.

Evt. kommentar til 3.2 Den registrertes rettigheter og friheter:

Vurdering av om den registrertes rettigheter er godt nok beskrevet:	
	Ok

3.3 Den registrertes friheter

Vurderinger rundt den registrertes friheter i forhold til Den europeiske menneskerettskonvensjonen (EMK).

Hvordan tar behandlingen hensyn til retten til privatliv og kommunikasjonsvern? (Viktig at den registrerte vurderer!)

Teieplikt for tilsette. Ein har rutiner og regler for at tilsette ikkje skal "snoke" i journaler.

Hvordan tar behandlingen hensyn til retten til ikke å bli diskriminert? (Viktig at den registrerte vurderer!)

Ein skal kun dokumentere informasjon som er relevant for behandling.

Hvordan tar behandlingen hensyn til retten til tanke-, tros- og religionsfrihet? (Viktig at den registrerte vurderer!)

Ein skal kun dokumentere informasjon som er relevant for behandling.

Hvordan tar behandlingen hensyn til retten til ytrings- og informasjonsfrihet? (Viktig at den registrerte vurderer!)

Teieplikt og informasjonsplikt for og frå tilsette.

Evt. kommentar til 3.3 Den registrertes friheter:

Vurdering av om den registrertes friheter er godt nok beskrevet:	
	Ok

Nedtrekksmeny
Nedtrekksmeny
Mangel/risiko

Konfidensialitet

Hvordan ivaretar behandlingen konfidensialiteten/fortroligheten til informasjonen om den registrerte, og hva kan det i verste fall føre til hvis informasjonen kommer uvedkommende i hende?			Risiko			Foreslåtte tekniske eller organisatoriske tiltak som vil kunne redusere risikoen for uønskede hendelser	Risiko etter tiltak		
Risikomomenter	**Konsekvens**	**Eksisterende tiltak**	**S**	**K**	**R**	**Anbefalte tiltak**	**S**	**K**	**R**
Uvedkomande kan lese på skjermen til tilsett, når den jobbar.	Får tilgang til særleg sensitive opplysingar.	Rutine for plassering av PC og PC-skjerm. Låst inn til vaktrom og andre kontor. Rutine for låsing av PC ved besøk på kontoret.	2	4	8	Drøfte problematikken i personalmøter. Gjere dei tilsette meir bevisst på risikoen for dette.	1	4	4
Forlet digitale verktøy ulåst.	Får tilgang til særleg sensitive opplysingar.	Har klistremerke på alle PC med påminning og visning på låsing av maskin. Har oppe temaet på personalmøte ofte. Har tilgang til e-læring gjennom Visma veiledar, som alle tilsette skal gjennom.	5	5	25	Få alle tilsette gjennom e-læringskursa. Rutine intern gjennomgang. Rutine for å ha inn ekstern person for gjennomgang.	3	5	15
Digitalt verktøy er hacket, eksempelvis via phishing.	Får tilgang til særleg sensitive opplysingar.	Følgje med på varslinger som kjem både internt og eksternt. Begrensa muligheit til å laste ned appar på mobilar for mobil omsorg.	2	5	10	Ha oppe temaet på personalmøte.	1	5	5
Tilsette med tilgang til fleire journal enn naudsynt, snoker i journal.	Får tilgang til særleg sensitive opplysingar.	Journaler skal vere tilgangsstyrt. Loggføring av aksessering av journaler. Rutine for tilsette som seier noko om når ein kan gå inn i ein journal, samt teieplikt. E-læringskurs.	2	5	10	Rutine for gjennomgang av logg. Ha oppe temaet på personalmøte. Få alle tilsette gjennom e-læringskursa.	1	5	5
Kollega "låner" ut sin tilgang.	Får tilgang til særleg sensitive opplysingar.	Tilsette låner ikkje ut tilgang, men låner ut innlogga PC for at den som manglar tilgang skal kunne skrive journal. "Utlånar" sitt ved siden av journalførar og tar over Pcen igjen ved fullført handling. Journalførar skal signere sitt eige namn i journalpost. Den som har lånt tilgang tar kontakt med systemansvarleg for resetting av brukaren sin.	3	1	3	Vidareføring av eksisterande tiltak. Ha oppe temaet på personalmøte.	3	1	3
Gjer informasjon til andre enn dei som har lov til å be om informasjon, eksempelvis pårørande som ikkje er nærmaste pårørande.	Får tilgang til særleg sensitive opplysingar.	Snakker jamnleg, til dels dagleg, om tematikken. Har arbeidsmøter der ein tar opp utfordringar. Har registrert i journal kven som er nærmaste pårørande, og skal ha informasjon.	3	4	12	Få alle tilsette gjennom e-læringskursa. Ha fokus på problematikken i personalmøte. Halde eksisterande tiltak vedlike.	2	4	8
Misbruk av spesialbegrunning for å få tilgang.	Får tilgang til særleg sensitive opplysingar.	Loggføring av aksessering av journaler. Rutine for tilsette som seier noko om når ein kan gå inn i ein journal, samt teieplikt. E-læringskurs.	2	5	10	Rutine for gjennomgang av logg. Ha oppe temaet på personalmøte. Få alle tilsette gjennom e-læringskursa.	1	5	5
Lite til ingen opplæring.	Noterer ting feil. Feil bruk av tilgang.	E-læringskurs. Har oppe temaet på personalmøtet. Opplæring av lærlinger. Rutine for journalføring.	3	3	9	Få alle tilsette gjennom e-læringskursa. Ha internkurs og opplæring.	2	3	6
Tar bilete av sår, eller personar, og liknande.	Bilete blir liggande på dei mobile einingane.	Rutine for å ta bilete via Profil (mobil omsorg). Fagleiar/leiar har rutine for å gjennomgå telefonar og eventuelt slette bilete. Rutine for å kun ta bilete av sår, for å ikkje ta bilete som identifiserer personen. Har temaet oppe på personalmøtet.	3	4	12	Få inn telefonar og nettbrett inn i Intune for å fjerne tilgang til kamera appen.	2	4	8
DBA -systemansvarleg logger inn som tilsett.	Får tilgang til særleg sensitive opplysingar, og kan hente ut eller endre på journaler i tilsette sitt namn.	Dei som har DBS tilgang må kun bruke tilgangen til systemarbeid.	1	4	4	Vidareføring av eksisterande tiltak.	1	4	4
Tilsette sluttar i arbeidsforhold, men beheld tilgangen sin til system.	Får tilgang til særleg sensitive opplysingar utan høveleg grunn. Kan potensielt hente ut og/eller spreie informasjon.	Rutine for å avslutte brukaren. På ferievikarer setter ein sluttdato, for automatisk avslutting av brukar. Loggføring av aksessering av journaler.	3	4	12	Årshjul for sjekk av brukarar. Rutine for gjennomgang av logg.	2	4	8

Integritet

Hvordan ivaretar behandlingen integriteten/riktigheten til informasjonen om den registrerte, og hva kan det i verste fall føre til hvis informasjonen er uriktig?			Risiko			Foreslåtte tekniske eller organisatoriske tiltak som vil kunne redusere risikoen for uønskede hendelser	Risiko etter tiltak		
Risikomomenter	**Konsekvens**	**Eksisterende tiltak**	**S**	**K**	**R**	**Anbefalte tiltak**	**S**	**K**	**R**
Lite til ingen opplæring.	Noterer ting feil. Feil bruk av tilgang.	Journalansvarleg kan rette, samt slette journalposter. E-læringskurs. Har oppe temaet på personalmøtet. Opplæring av lærlinger. Rutine for journalføring.	2	3	6	Få alle tilsette gjennom e-læringskursa.	2	3	6
Journalfører personleg vurdering av brukar og pårørande, som ikkje er knytt til tenesteyting.	Feil i journal knytt til fagutøvelse.	E-læringskurs. Rutine for journalføring. Har det oppe som tema i personalmøte.	2	3	6	Få alle tilsette gjennom e-læringskursa.	2	3	6
					0				0
					0				0
					0				0

Tilgjengelighet

Hvordan ivaretar behandlingen tilgjengeligheten til informasjonen om den registrerte, og hva kan det i verste fall føre til hvis informasjonen ikke er tilgjengelig?			Risiko			Foreslåtte tekniske eller organisatoriske tiltak som vil kunne redusere risikoen for uønskede hendelser	Risiko etter tiltak		
Risikomomenter	**Konsekvens**	**Eksisterende tiltak**	**S**	**K**	**R**	**Anbefalte tiltak**	**S**	**K**	**R**
Straumstans.	Får ikkje tilgang til naudsynt helseopplysing. Får ikkje effektiv samhandling med samhandlingspartar. Får ikkje dokumentert i sanntid.	Aggregat på lokasjon. Mobile einingar. Skriftlige prosedyrer ved straumstans.	5	2	10	Vidareføring av eksisterande tiltak.	5	2	10
Utfall av nett-tilgang.	Får ikkje tilgang til naudsynt helseopplysing. Får ikkje effektiv samhandling med samhandlingspartar. Får ikkje dokumentert i sanntid.	Skriftlege prosedyrar. Papir og blyant, mobil dekning også skal vere ute. Mobile einingar. Ta kontakt med IKT.	1	4	4	Vidareføring av eksisterande tiltak.	1	4	4
Server utav drift.	Får ikkje tilgang til naudsynt helseopplysing. Får ikkje effektiv samhandling med samhandlingspartar. Får ikkje dokumentert i sanntid.	Papir og blyant. Skriftlege prosedyrar. Vakttelefon som sjukehus skal kunne kontakte via. Ha kontakt med IKT/Leverandør.	1	4	4	Vidareføring av eksisterande tiltak.	1	4	4
Dødsoner i mobildekning.	Får ikkje tilgang til naudsynt helseopplysing. Får ikkje effektiv samhandling med samhandlingspartar. Får ikkje dokumentert i sanntid.	Flytte seg til nærmaste dekning.	1	4	4	Vidareføring av eksisterande tiltak.	1	4	4
Utfall av mobildekning.	Får ikkje tilgang til naudsynt helseopplysing. Får ikkje effektiv samhandling med samhandlingspartar. Får ikkje dokumentert i sanntid.	Nytte PC. Skriftlege prosedyrar. Ha kontakt med Telenor (sjekke driftsmelding).	1	2	2	Vidareføring av eksisterande tiltak.	1	2	2

Åpenhet

Hvordan ivaretar behandlingen åpenheten rundt informasjonen om den registrerte, og hvilke konsekvenser kan det få for den registrertes personvern om tilstrekkelig informasjon ikke er gitt?			Risiko			Foreslåtte tekniske eller organisatoriske tiltak som vil kunne redusere risikoen for uønskede hendelser	Risiko etter tiltak		
Risikomomenter	**Konsekvens**	**Eksisterende tiltak**	**S**	**K**	**R**	**Anbefalte tiltak**	**S**	**K**	**R**
Systemet er lukka for den registrerte.	Får i utgangspunktet ikkje innsyn i eigne opplysingar.	Alle har rett til innsyn. Viser til lovverk i vedtak, samt eit vedlegg om retten til innsyn.	3	3	9	Ha alle tilsette gjennom e-læringskurs. Bevisstgjering av tilsette.	2	3	6
Den registrerte får ikkje vete kva som blir lagra om seg.	Pasient/den registrerte vegrar seg for å sei enkelte detaljer i tru om at det blir registrert i negativ forstand.	Forvaltning levere ut eit skriv om Iplos-registrering. Vedlegg til vedtak om korleis og kva som blir registert om pasienten. Samt kva som kan bli delt med eksempelvis spesialist helsetenester.	2	3	6	Ha alle tilsette gjennom e-læringskurs. Bevisstgjering av tilsette.	2	3	6
Pårørande sender inn melding, men ynskjer å ikkje bli oppgitt i journal.		Melding blir journalført med notat om å ikkje gje dette ut ved innsyn.	2	3	6	Ha alle tilsette gjennom e-læringskurs. Bevisstgjering av tilsette.	2	3	6
					0				0
					0				0

Forutsigbarhet

I hvilken grad er kompleksiteten/uforutsigbarheten i behandlingen høy og tilsvarende vanskelig for den registrerte å forstå, og hvilke konsekvenser kan det få for den registrertes personvern om kompleksiteten av behandlingen ikke er gitt eller forstått?			Risiko			Foreslåtte tekniske eller organisatoriske tiltak som vil kunne redusere risikoen for uønskede hendelser	Risiko etter tiltak		
Risikomomenter	**Konsekvens**	**Eksisterende tiltak**	**S**	**K**	**R**	**Anbefalte tiltak**	**S**	**K**	**R**
Nyttar fagspråk.	Pasient/pårørande skjønar ikkje kva det er snakk om.	E-læringskurs. Bevisstgjering av tilsette.	2	2	4	Vidareføring av eksisterande tiltak.	2	2	4
Kompleks struktur i profil, som gjer det utfordrande for pasient/pårørande å lese journal.	Pasient/pårørande skjønar ikkje kva det er snakk om.	E-læringskurs. Bevisstgjering av tilsette.	3	2	6	Vidareføring av eksisterande tiltak. Ta i bruk Visma flyt.	2	2	4
Tilsette fører inn opplysingar forskjellige stader i profil.	Tilsette finn ikkje/ får ikkje med seg opplysinger. Feil i rapport.	E-læringskurs. Bevisstgjering av tilsette.	3	2	6	Vidareføring av eksisterande tiltak. Ta i bruk Visma flyt.	2	2	4
					0				0
					0				0

Medbestemmelse

Hvordan ivaretar behandlingen den registrertes muligheter for medbestemmelse/påvirkning, og hvilke konsekvenser kan det få for den registrertes personvern om den ikke har dette?			Risiko			Foreslåtte tekniske eller organisatoriske tiltak som vil kunne redusere risikoen for uønskede hendelser	Risiko etter tiltak		
Risikomomenter	**Konsekvens**	**Eksisterende tiltak**	**S**	**K**	**R**	**Anbefalte tiltak**	**S**	**K**	**R**
Systemet er lukka for den registrerte.	Får i utgangspunktet ikkje innsyn i eigne opplysingar.	Den registrerte må be om innsyn. Viser til lovverk i vedtak, samt eit vedlegg om retten til innsyn.	3	3	9	Ha alle tilsette gjennom e-læringskurs. Bevisstgjering av tilsette.	2	3	6
Den registrerte får ikkje vete kva som blir lagra om seg.	Pasient/den registrerte vegrar seg for å sei enkelte detaljer i tru om at det blir registrert i negativ forstand.	Forvaltning levere ut eit skriv om Iplos-registrering.	2	3	6	Informasjon til den registrete om det skulle vere noko som ser ut til å ver feil, kan dei kontakte tenesta, og be om endring/sletting. Det er ikkje alt som kan endrast eller slettast.	2	3	6
					0				0
					0				0
					0				0

Friheter

Vurder hvordan de registrertes friheter i forhold til Den europeiske menneskerettskonvensjonen (EMK) er tatt hensyn til. Retten til privatliv og kommunikasjonsvern, retten til ikke å bli diskriminert, tanke-, tros- og religionsfrihet, ytrings- og informasjonsfrihet			Risiko			Foreslåtte tekniske eller organisatoriske tiltak som vil kunne redusere risikoen for uønskede hendelser	Risiko etter tiltak		
Risikomomenter	**Konsekvens**	**Eksisterende tiltak**	**S**	**K**	**R**	**Anbefalte tiltak**	**S**	**K**	**R**
Dagens system klarar ikkje å skilje mellom hen og han/ho.	Kan føle seg diskriminert.	Kan endre til det til det kjannet dei identifiserer seg med. System støtter ikkje hen, og usikkert om nytt system vil gjere det.	1	3	3	Vidareføring av eksisterande tiltak.	1	3	3
Reservasjonar blir ikkje registrert.	Får eksempelvis blodoverføring, HLR-, eller mat hen ikkje skal ha.	Brukar/pårørande skal informere om dette i møte/samtale. Rutine for å sette dette i fagsystem.	2	4	8	Vidareføring av eksisterande tiltak.	2	4	8
Samtykke knytt til reservasjoner blir ikkje registrert.	Kan få hjelp og tiltak hen ikkje ynskjer.	Brukar/pårørande skal bli informert om dette i møte. Rutine for å sette dette i fagssystem.	2	4	8	Vidareføring av eksisterande tiltak.	2	4	8
					0				0
					0				0

Behandlingen - Etter gjennoførte tiltak	
Ny beskrivelse av behandlingen	Dersom tiltak bestemmes iverksatt og behandlingen endres, tegn evt. nytt flytskjema og legg inn i samme fil som det opprinnelige flytskjemaet. Lagre flytskjemaet eks. som: "ÅÅÅÅ-MM-DD DPIA for behandlingsnavn - Vedlegg A" eller kopiér skissen til arkfanen "Skisse" i dette dokumentet.

Risikotabell - må være forankret i ledelsen

Bærum kommune - risikotabell						
		Ubetydelig konsekvens	Liten konsekvens	Moderat konsekvens	Alvorlig konsekvens	Katastrofal konsekvens
		1	2	3	4	5
Svært høy sannsynlighet	5	Moderat (5)	Moderat (10)	Høy (15)	Katastrofal (20)	Katastrofal (25)
Høy sannsynlighet	4	Lav (4)	Moderat (8)	Høy (12)	Høy (16)	Katastrofal (20)
Moderat sannsynlighet	3	Lav (3)	Moderat (6)	Moderat (9)	Høy (12)	Høy (15)
Liten sannsynlighet	2	Lav (2)	Lav (4)	Moderat (6)	Moderat (8)	Moderat (10)
Svært liten sannsynlighet	1	Lav (1)	Lav (2)	Lav (3)	Lav (4)	Moderat (5)

Sannsynlighet		
Nivå	**Beskrivelse**	**Veiledning**
1	Det er svært lite sannsynlig at hendelsen vil inntreffe.	Inntreffer sjeldnere enn årlig og/eller ingen kjente sårbarheter/trusler.
2	Det er lite sannsynlig at hendelsen vil inntreffe.	Inntreffer årlig høyst årlig og/eller få eller ingen kjente sårbarheter/trusler.
3	Det er moderat sannsynlig at hendelsen vil inntreffe.	Inntreffer høyst månedlig og/eller kjente mindre alvorlige sårbarheter/trusler.
4	Det er sannsynlig at hendelsen vil inntreffe.	Inntreffer ukentlig og/eller kjente alvorlige sårbarheter/trusler.
5	Det er høy sannsynlighet for at hendelsen vil inntreffe.	Inntreffer daglig og/eller svært alvorlige kjente sårbarheter/trusler.

Konsekvens		
Nivå	**Beskrivelse**	**Veiledning**
1	Den aktuelle konsekvensen for den registrertes personvern, anseelse og/eller personlig integritet vurderes som ubetydelig.	- Hendelsen kan føre til forbigående, mindre økonomisk tap for den registrerte. - Hendelsen kan føre til midlertidig og begrenset tap av den registrertes omdømme. - Hendelsen kan føre til at den registrertes rett til personvern ikke er tilstrekkelig ivaretatt i en svært kort periode og uten å involvere særlige kategorier/sårbare grupper.
2	Den aktuelle konsekvensen for den registrertes personvern, anseelse eller personlig integritet er lav, kan vurderes som noe krenkende og/eller påvirker helse i noen grad.	- Hendelsen kan føre til midlertidige eller mindre alvorlige helsemessige konsekvenser for den registrerte. - Hendelsen kan føre til forbigående økonomisk tap for den registrerte. - Hendelsen kan føre til midlertidig eller begrenset tap av den registrertes omdømme. - Hendelsen kan føre til at den registrertes rett til personvern ikke er tilstrekkelig ivaretatt i en svært kort periode eller uten å involvere særlige kategorier/sårbare grupper. - Den registrertes tillit til kommunen utfordres midlertidig.
3	Den aktuelle konsekvensen for den registrertes personvern, anseelse eller personlig integritet er moderat, kan oppfattes som krenkende og/eller påvirker helse.	- Hendelsen kan føre til midlertidige eller noe mer alvorlige helsemessige konsekvenser for den registrerte. - Hendelsen kan føre til økonomisk tap av noe varighet for den registrerte. Hendelsen kan føre til midlertidige eller noe mer alvorlige tap av den regis- trertes omdømme. - Hendelsen kan føre til at den registrertes rett til personvern krenkes noe mer alvorlig. - Den registrertes tillit til kommunen utfordres.
4	Den aktuelle konsekvensen for den registrertes personvern er alvorlig, anseelse eller personlig integritet, kan oppfattes som svært krenkende og/eller påvirker helse i stor grad.	- Hendelsen kan føre til varige eller alvorlige helsemessige konsekvenser for den registrerte. - Hendelsen kan føre til økonomisk tap av betydelig varighet for den registrerte. - Hendelsen kan føre til varig eller alvorlig tap av den registrertes omdømme. - Hendelsen kan føre til at den registrertes rett til personvern krenkes alvorlig. - Den registrerte taper tillit til kommunen.
5	Den aktuelle konsekvensen for den registrertes personvern, anseelse eller personlig integritet er svært alvorlig, kan oppfattes som svært krenkende og/eller kan medføre tap av liv.	- Hendelsen kan føre til tap av liv (for den registrerte). - Hendelsen kan føre til varige og alvorlige helsemessige konsekvenser for den registrerte. - Hendelsen kan føre til varig og betydelig økonomisk tap for den registrerte. - Hendelsen kan føre til varig og alvorlig tap av den registrertes omdømme. - Hendelsen kan føre til at den registrertes rett til personvern krenkes på en svært alvorlig måte. - Den registrerte og samfunnet taper tillit til kommunen.

Rapport - Data Protection Impact Assessment

(Skal, med få unntak, være offentlig tilgjengelig)

(1) Innledende informasjon

(Innhentet fra tidligere arkfaner)

Navn på tjeneste	**Pleie- og Omsorgssystem - Visma PROFIL**
Behandling	**Elektronisk journal system for Helse/Pleie og omsorg.**
Formål	**Sikre forsvarleg helsehjelp.**
Behandlingsgrunnlag	**Oppfylle rettslig forpliktelse (lov) (art. 6.1 c)**
Hjemmel	**Journalforskrifta.**
Kommentarer	**0**

Konklusjon initiell vurdering:	**Ja/Nei**
Det er to "Ja" eller flere, det vurderes derfor at det er sannsynlig at behandlingen vil innbære en høy risiko for fysiske personers personvern, deres rettigheter og friheter - full DPIA skal gjennomføres	

(2) Vurdering av Systematisk beskrivelse

(Innhentet fra tidligere arkfaner)

Behandlingens formål	**0**
Behandlingens grunnlag	**0**
Behandlingens art	**0**
Behandlingens omfang	
Konteksten behandlingen utføres i	**Godt nok beskrevet**
Innebygd personvern	**0**
Bruk av databehandler	**0**
Tekniske og organisatoriske sikkerhetstiltak	**Få oppdatert og godkjent prosedyrer når det gjeld tilgangsstyring og oppfølging på dette området.**

(3) Vurdering av Nødvendighet og proporsjonalitet

(Innhentet fra tidligere arkfaner)

Personvernprinsippene	**0**
Den registrertes rettigheter	**0**
Den registrertes friheter	**0**

(4) Risikoer og (5) tiltak som må/bør vurderes

(Innhentet fra tidligere arkfaner)

Område	Risikomomenter	Risiko S	K	R	Anbefalte tiltak	Ansvarlig for oppfølgning	Frist	Risiko S	K	R
Konfidensialitet	Uvedkomande kan lese på skjermen til tilsett, når den jobbar.	2	4	8	Drøfte problematikken i personalmøter. Gjere dei tilsette meir bevisst på risikoen for dette.			1	4	4
Konfidensialitet	Forlet digitale verktøy ulåst.	5	5	25	Få alle tilsette gjennom e-læringskursa. Rutine intern gjennomgang. Rutine for å ha inn ekstern person for gjennomgang.			3	5	15
Konfidensialitet	Digitalt verktøy er hacket, eksempelvis via phishing.	2	5	10	Ha oppe temaet på personalmøte.			1	5	5
Konfidensialitet	Tilsette med tilgang til fleire journal enn naudsynt, snoker i journal.	2	5	10	Rutine for gjennomgang av logg. Ha oppe temaet på personalmøte. Få alle tilsette gjennom e-læringskursa.			1	5	5
Konfidensialitet	Kollega "låner" ut sin tilgang.	3	1	3	Vidareføring av eksisterande tiltak. Ha oppe temaet på personalmøte.			3	1	3
Konfidensialitet	Gjer informasjon til andre enn dei som har lov til å be om informasjon, eksempelvis pårørande som ikkje er nærmaste pårørande.	3	4	12	Få alle tilsette gjennom e-læringskursa. Ha fokus på problematikken i personalmøte. Halde eksisterande tiltak vedlike.			2	4	8
Konfidensialitet	Misbruk av spesialbegrunning for å få tilgang.	2	5	10	Rutine for gjennomgang av logg. Ha oppe temaet på personalmøte. Få alle tilsette gjennom e-læringskursa.			1	5	5
Konfidensialitet	Lite til ingen opplæring.	3	3	9	Få alle tilsette gjennom e-læringskursa. Ha internkurs og opplæring.			2	3	6
Konfidensialitet	Tar bilete av sår, eller personar, og liknande.	3	4	12	Få inn telefonar og nettbrett inn i Intune for å fjerne tilgang til kamera appen.			2	4	8
Konfidensialitet	Tilsette sluttar i arbeidsforhold, men beheld tilgangen sin til system.	3	4	12	Årshjul for sjekk av brukarar. Rutine for gjennomgang av logg.			2	4	8

Område	Risikomomenter	Risiko S	K	R	Anbefalte tiltak	Ansvarlig for oppfølgning	Frist	Risiko S	K	R
Integritet	Lite til ingen opplæring.	2	3	6	Få alle tilsette gjennom e-læringskursa.			2	3	6
Integritet	Journalfører personleg vurdering av brukar og pårørande, som ikkje er knytt til tenesteyting.	2	3	6	Få alle tilsette gjennom e-læringskursa.			2	3	6
Integritet	0	0	0	0	0			0	0	0
Integritet	0	0	0	0	0			0	0	0
Integritet	0	0	0	0	0			0	0	0

Område	Risikomomenter	Risiko S	K	R	Anbefalte tiltak	Ansvarlig for oppfølgning	Frist	Risiko S	K	R
Tilgjengelighet	Straumstans.	5	2	10	Vidareføring av eksisterande tiltak.			5	2	10
Tilgjengelighet	Utfall av nett-tilgang.	1	4	4	Vidareføring av eksisterande tiltak.			1	4	4
Tilgjengelighet	Server utav drift.	1	4	4	Vidareføring av eksisterande tiltak.			1	4	4
Tilgjengelighet	Dødsoner i mobildekning.	1	4	4	Vidareføring av eksisterande tiltak.			1	4	4
Tilgjengelighet	Utfall av mobildekning.	1	2	2	Vidareføring av eksisterande tiltak.			1	2	2

Område	Risikomomenter	Risiko S	K	R	Anbefalte tiltak	Ansvarlig for oppfølgning	Frist	Risiko S	K	R
Åpenhet	Systemet er lukka for den registrerte.	3	3	9	Ha alle tilsette gjennom e-læringskurs. Bevisstgjering av tilsette.			2	3	6
Åpenhet	Den registrerte får ikkje vete kva som blir lagra om seg.	2	3	6	Ha alle tilsette gjennom e-læringskurs. Bevisstgjering av tilsette.			2	3	6
Åpenhet	Pårørande sender inn melding, men ynskjer å ikkje bli oppgitt i journal.	2	3	6	Ha alle tilsette gjennom e-læringskurs. Bevisstgjering av tilsette.			2	3	6
Åpenhet	0	0	0	0	0			0	0	0
Åpenhet	0	0	0	0	0			0	0	0

Område	Risikomomenter	Risiko S	K	R	Anbefalte tiltak	Ansvarlig for oppfølgning	Frist	Risiko S	K	R
Forutsigbarhet	Nyttar fagspråk.	2	2	4	Vidareføring av eksisterande tiltak.			2	2	4
Forutsigbarhet	Kompleks struktur i profil, som gjer det utfordrande for pasient/pårørande å lese journal.	3	2	6	Vidareføring av eksisterande tiltak. Ta i bruk Visma flyt.			2	2	4
Forutsigbarhet	Tilsette fører inn opplysingar forskjellige stader i profil.	3	2	6	Vidareføring av eksisterande tiltak. Ta i bruk Visma flyt.			2	2	4
Forutsigbarhet	0	0	0	0	0			0	0	0
Forutsigbarhet	0	0	0	0	0			0	0	0

Område	Risikomomenter	Risiko S	K	R	Anbefalte tiltak	Ansvarlig for oppfølgning	Frist	Risiko S	K	R
Medbestemmelse	Systemet er lukka for den registrerte.	3	3	9	Ha alle tilsette gjennom e-læringskurs. Bevisstgjering av tilsette.			2	3	6
Medbestemmelse	Den registrerte får ikkje vete kva som blir lagra om seg.	2	3	6	Informasjon til den registrete om det skulle vere noko som ser ut til å ver feil, kan dei kontakte tenesta, og be om endring/sletting. Det er ikkje alt som kan endrast eller slettast.			2	3	6
Medbestemmelse	0	0	0	0	0			0	0	0
Medbestemmelse	0	0	0	0	0			0	0	0
Medbestemmelse	0	0	0	0	0			0	0	0

Område	Risikomomenter	Risiko S	K	R	Anbefalte tiltak	Ansvarlig for oppfølgning	Frist	Risiko S	K	R
Friheter	Dagens system klarar ikkje å skilje mellom hen og han/ho.	1	3	3	Vidareføring av eksisterande tiltak.			1	3	3
Friheter	Reservasjonar blir ikkje registrert.	2	4	8	Vidareføring av eksisterande tiltak.			2	4	8
Friheter	Samtykke knytt til reservasjoner blir ikkje registrert.	2	4	8	Vidareføring av eksisterande tiltak.			2	4	8
Friheter	0	0	0	0	0			0	0	0
Friheter	0	0	0	0	0			0	0	0

Bærum kommune - risikotabell

		Ubetydelig konsekvens 1	Liten konsekvens 2	Moderat konsekvens 3	Alvorlig konsekvens 4	Katastrofal konsekvens 5
Svært høy sannsynlighet	5	Moderat (5)	Moderat (10)	Høy (15)	Katastrofal (20)	Katastrofal (25)
Høy sannsynlighet	4	Lav (4)	Moderat (8)	Høy (12)	Høy (16)	Katastrofal (20)
Moderat sannsynlighet	3	Lav (3)	Moderat (6)	Moderat (9)	Høy (12)	Høy (15)
Liten sannsynlighet	2	Lav (2)	Lav (4)	Moderat (6)	Moderat (8)	Moderat (10)
Svært liten sannsynlighet	1	Lav (1)	Lav (2)	Lav (3)	Lav (4)	Moderat (5)

Mørk rødt:
Strakstiltak. (Meget kritisk = fare for liv og helse)
Rødt:
Tiltak må iverksettes – utarbeid tiltaksplan
Gult:
Det må vurderes om tiltak skal iverksettes
Grønt:
Ikke nødvendig å iverksette tiltak

(6) Vurdering og synspunkter til behandlingen og dens risikoer (restrisiko):

Behandlingsansvarliges vurdering:	**Blitt meir bevisst omfang og risikoar. Ser at me jobbar likt og må jobbe felles for å ivareta personvernet. Må være bevisst og jobbe med ulike risikoområder jevnlig.**
Den registrertes vurdering:	**Greit å få delta i prosessen. Interessant.**
Personvernombudets vurdering:	**Det har vert nokre gode diskusjoner i løpet av denne DPIAen og ROSen. Det har også vert ting som har måtte blitt avklart mellom møta interkommunalt, rundt funksjoner og logging.** **Om tiltak er og blir gjennomført ser eg for meg at det skal skje minimalt med feil, og at dataen skal ligge trygt.** **Når ein har fått henta inn synspunkt frå den registrerte så vil eg sei at dette er eit godt utarbeida dokument.** **Om kommuner som ikkje har vert med i utarbeidinga på denne (samt dei som har vert med) har lasta dokumentet ned og fått gjort sine tilpassingar, samt henta synspunkt frå den registrerte, så anser eg dokumentet som fullført fram til revisjon.**
Andre representanters vurdering:	

Konklusjon fra deltakere (velg fra nedtrekkslisten):	***Ja/Nei***
Deltakende parter er enige om at behandlingen kan gjennomføres, forutsatt at nevnte tiltak iverksettes og følges opp	

(7) Ledelsens validering av DPIA

Ledelsens vurdering av risikobildet

Ledelsen vurderer anbefalte tiltak, restrisiko og beslutter handlingsplan

Beskriv: Ledelsens vurdering av risiko

Konklusjon fra ledelsen	
Ledelsen beslutter og begrunner om DPIA er (velg fra nedtrekkslisten) :	***Ja/Nei***
- Velg -	

Behandlingsansvarliges signatur/dato (benyttes ved full DPIA):

Signatur/dato:

2.4 Behandlingens omfang - Skisse med dataflyt

Helsepersonell registrerar opplysningar om pasient/brukar i EPJ.

Innbygger dialog (ikkje aktivert ennå)

Visma Profil

Ved innleggelsar er det e-meldingsutveksling mellom Helse-og omsorg og spesialisthelsetenesten som vert sendt og lagra i EPJ.

NHN person register-tenesten

IPLOS opplysningar til KRP

Visma mobil omsorg

E-meldingsutveksling skjer mellom fastlege og sjukepleietenesten /psykisk helseteneste og fysioterapitenesten. Alt vert lagra i EPJ.

Kjernejournal

Visma saksarkiv

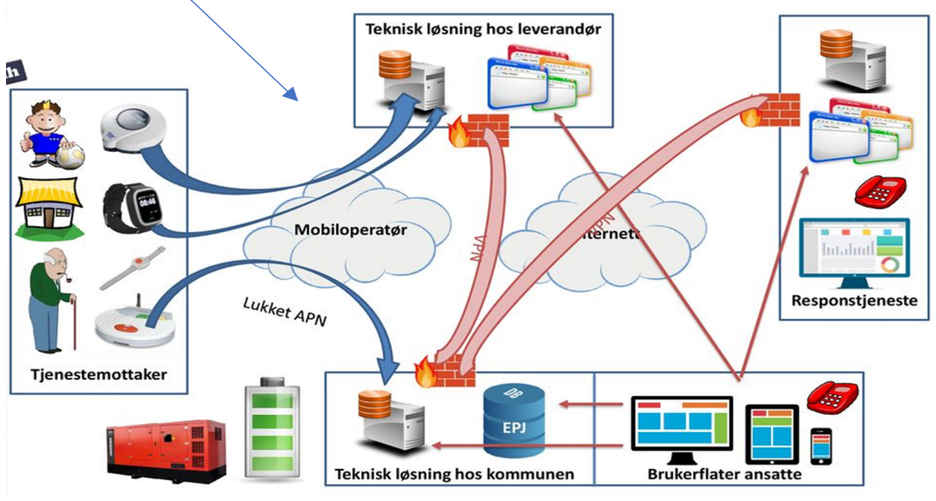
KS svar ut

Økonomi og oppgjørtenesten sender inntektsforepørsel til NAV via e-meldingssystemet og får svar tilbake frå NAV

Rute planlegger

All meldingsutveksling skjer på sikker måte via meldingstenaren Visma Link.

Flyskjema frå IKTNH som driftar IKT systema:



DPIA - Møte/endringslogg				
Versjon	**Dato**	**Endringsbeskrivelse**	**Endret av**	**Deltakere**

Lenker til omtalte referanser	
Personopplysningsloven	https://lovdata.no/dokument/NL/lov/2018-06-15-38
Datatilsynets MÅ -liste	https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/
Personopplysningsloven, artikkel 35	https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_35#gdpr/ARTIKKEL_35
Personopplysningsloven, artikkel 5	https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_5#gdpr/ARTIKKEL_5
Personopplysningsloven, artikkel 9	https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_9#gdpr/ARTIKKEL_9
Personopplysningsloven, artikkel 10	https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_10#gdpr/ARTIKKEL_10
Personopplysningsloven, artikkel 6	https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_6#gdpr/ARTIKKEL_6
Innebygd personvern	https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-
Den europeiske menneskerettighetskonvensjon (EMK)	https://www.regjeringen.no/no/tema/utenrikssaker/menneskerettigheter/id1160/

Vedlegg til DPIA				