Data Protection Impact Assessment (DPIA) – Personvernkonsekvensutredning etter GDPR

Denne malen er utviklet på bakgrunn av krav i GDPR. Det er tatt hensyn til Datatilsynets veiledning om DPIA. En del av teksten er hentet fra Datatilsynets sjekkliste for vurdering av personvernkonsekvenser. Malen gir et bilde av momentene som **bør** vurderes i en DPIA. Den enkelte virksomhet som bruker malen må selv konkret vurdere innhold og omfang av egen DPIA. Tabellene i malen er ikke uttømmende og må tilpasses de enkelte behandlingene som omfattes av en DPIA.

DEL I. Vurdering av behov for DPIA

[I denne delen er det kun nødvendig å besvare spørsmålene i tabellen nedenfor, ingen analyse.]

Når må DPIA gjennomføres?

> *«Dersom det er sannsynlig at en **type behandling**, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens **art, omfang, formål og sammenhengen den utføres i**, vil medføre en **høy risiko** for fysiske personers **rettigheter og friheter**, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for vernet av personopplysninger.»* (GDPR art.35.1)

Kriterier når DPIA *kan* bli et krav:

1. **Evaluering eller scoring**, spesielt knyttet til arbeidsresultater, økonomisk situasjon, helse, personlige preferanser eller interesser, oppførsel og adferd, lokasjon og bevegelser osv.
2. **Automatiserte beslutninger** med juridisk eller tilsvarende betydning.
3. **Systematisk overvåking** av registrerte.
4. **Særlige kategorier personopplysninger** eller **andre sensitive personopplysninger av høy personlig karakter** (sistnevnte spesielt knyttet de enkeltes «friheter», men kan også omfatte f.eks. økonomiske og finansielle opplysninger).
5. **Databehandling i stort omfang**, som at det er et stort antall registrerte involvert, store mengder data, mange ulike typer data, lang varighet av behandlingen, stor geografisk utbredelse av behandlingen osv.
6. **Kombinering eller sammenstilling av datasett**.

7. Personopplysninger vedrørende **spesielt sårbare registrerte** (som barn, ansatte, psykisk syke, asylsøkere, eldre, pasienter mv.).
8. **Innovativ eller nyskapende bruk av personopplysninger,** som f.eks. bruk av biometriske data for tilgangskontroll, Internet of Things-løsninger, velferdsteknologi osv.
9. Når behandlingen i seg selv **forhindrer eller begrenser de registrertes mulighet til å utøve sine rettigheter** etter loven eller avtale, eller **bruke tjenester**.

Vurderingsspørsmål om behov for DPIA: Visma Familia - barnevern

Nr.	Vurderingsspørsmål	Ja/Nei
1.	Er dette et nytt prosjekt eller prosess?	ja
2.	Vil prosjektet innebære innsamling av ny informasjon om enkeltpersoner?	ja
3.	Vil prosjektet be enkeltpersoner om å gi informasjon om seg selv?	ja
4.	Vil informasjon om enkeltpersoner bli delt med organisasjoner eller personer som ikke tidligere har hatt rutinemessig tilgang til informasjonen?	nei
5.	Skal du bruke informasjon om enkeltpersoner som er innsamlet for et formål, men der opplysningene for tiden ikke er eller ikke lenger er i bruk (ikke behandles utover lagring)?	ja
6.	Innebærer prosjektet at du bruker ny teknologi som kan oppfattes som inngripende for personvernet? For eksempel, bruk av biometri eller ansiktsgjenkjenning?	nei
7.	Vil prosjektet resultere i at du tar beslutninger eller gjennomfører tiltak mot enkeltpersoner på måter som kan ha en betydelig innvirkning på dem?	ja
8.	Basert på typen informasjon om enkeltpersoner, er det spesielt sannsynlig at bekymringen for eller forventninger til personvernet vil øke?	ja
9.	Vil prosjektet kreve at du kontakter personer på måter som de kan finne inngripende?	ja

Dersom svaret er "ja" på ett eller flere av spørsmålene ovenfor, kan det bety at det er behov for DPIA. Forsett til DEL II.

DEL II. Grunnleggende utgangspunkter og beskrivelser

II.1. Bakgrunn

- Forutsetninger og avgrensning
  DPIA for Visma Familia
- Hvem som deltar i DPIA (DPIA-team)
  Trude Hagland, Ranja Abrahamsen, Anne Grethe Solbu og Mona Lilleng samt personvernombud Bjørn Nilsen
- Interessenter
  Barneverntjenestens klienter og samarbeidspartnere

II.2. Løsning, tjeneste og system

- Beskrivelse av løsning, tjeneste og system (eller konsept)
  Beskrivelsen bør omfatte: informasjonssystem, infrastruktur, tjenester, driftsmiljø og ytre grenser, informasjonssystemets tilstøtende grensesnitt med andre systemer og hvordan personopplysningene flyter (overføres mellom ulike systemer).

- Beskrivelse av behandling av personopplysninger i løsning, tjeneste og system (inkl. informasjonsflyt)
  Beskrivelsen bør omfatte et helhetlig og fullstendig bilde av prosesser og tilknyttede aktiva (maskinvare, programvare, nettverk, personer, papir, kommunikasjonskanaler med videre) som er nødvendige for hele livssyklusen til personopplysninger (fra innsamling til sletting).
  - Fullelektronisk dokumentbehandling, med svar inn/ut tjeneste i fagsystemet.
  - Papirdokumenter skannes inn til fagsystemet. Det er utarbeidet egne retningslinjer for dette. Det er i tillegg utarbeidet arkivplan for sikker sone.

II.3. Behandlingens omfang

- Beskrivelse av alle opplysninger som behandles
  - hvilke typer opplysninger (særlige kategorier eller ikke)
    - Personopplysninger underlagt lovbestemt taushetsplikt
    - Sensitive personopplysninger
- Kategorier av de registrerte (for eksempel barn, foreldre, pasienter, ansatte osv.)
  - Foreldre
  - Barn
  - Øvrig familie ved samtykke til registrering

- Volumet av data (antall variabler, detaljeringsgrad).
  - Omfang vurderes i den enkelte sak. Sakens omfang skal ikke gjøres større enn nødvendig for å belyse saken god nok.
- Frekvensen av behandlingen (om opplysningene innhentes en gang, flere ganger, regelmessig, kontinuerlig, og så videre).
  - Ved behov samles opplysninger inn flere ganger. Avgrenset periode innenfor undersøkelsestiden.
- Det geografiske omfanget (lokalt, regionalt, nasjonalt, internasjonalt, globalt).
  - Lokalt og nasjonalt

II.4. Formålsbeskrivelser

- Beskrivelse av formålet med behandlingen av personopplysninger
  [Det må presiseres:
  - Formålet med hele løsningen
  - Formålet med behandling av personopplysninger i løsningen generelt
  - Formålet med detaljerte typer av behandlingsaktiviteter dersom de har ulike formål]

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Hva er formålet med behandlingen?	Oppbevare klientinformasjon. Undersøke barns omsorgssituasjon og vurdering av tiltak
2.	Vil formålet være å treffe avgjørelser om enkeltpersoner basert på systematisk og omfattende analyse av personlige aspekter?	Ja. Kartlegger familiesituasjoner og deres behov for bistand etter barnevernloven.
3.	Vil behandlingen av personopplysninger ha som mål å ta beslutninger som får betydning for den registrerte?	Ja. Tilbud om ulike tiltak eller omsorgsovertakelse.
4.	Skal opplysningene brukes til å profilere den registrerte?	NEI.
5.	Brukes personopplysninger for å avdekke ukjente sider eller for å gjenkjenne mønstre ved den registrerte?	Ja. Atferd, relasjoner, omsorgsevne/behov

DEL III. Behandlingens lovlighet

III.1. Hjemmelsgrunnlag

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Finnes det hjemmelsgrunnlag i forskrift eller lov for behandlingen av personopplysninger?	Barnevernloven, forvaltningsloven, samt personvernforordningen artikkel 6 c, e og 9 a, b
2.	Finnes det annet rettsgrunnlag for behandlingen (for eksempel samtykke, avtale, verne vitale interesser, utførelse av myndighetsoppgave, oppfylle rettslig forpliktelse, jf. GDPR art.6)?	Jf pkt. 1.
3.	Finnes det konsesjon eller forhåndsgodkjenning fra REK eller Datatilsynet, eller dispensasjon fra taushetsplikten?	

- Gjennomgang av rettsgrunnlag, konsesjoner og dispensasjoner.
- Gjennomgang av begrensninger eller mulighetsrom som rettsgrunnlag, konsesjoner eller dispensasjoner gir.

III.2. Samtykke

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Forutsettes det samtykke for behandlingen?	Nei ikke i alle tilfeller. Hjemmel i lov. Det jobbes for involvering av den registrerte. Ved frivillige hjelpetiltak etter fylte 18 år. Ved vedtak om frivilligplassering §4-4, 6. eller 4-24 frivilligplassering av ungdom i institusjon forutsettes samtykke. Trekkes samtykket, kan det resultere i rettslig behandling – art 6 c.
2.	Hvordan vil samtykke bli innhentet?	Samtykke signering i direkte tilknytning til vedtak, med nødvendig informasjon om partens rettigheter og vår håndtering av saken.

Nr.	Vurderingsspørsmål	Svar (forklar svar)
3.	Er alle kravene til samtykke oppfylt? Samtykke fra den registrerte må være frivillig, spesifikk, informert og utvetydig (GDPR art.4).	Ja. Beskrivelser av mulighet for å trekke samtykke og hva som kan bli utfallet av trukket samtykke beskrives og leses opp til den registrerte.
4.	Dokumenteres samtykke?	JA
5.	Kan samtykke trekkes tilbake like enkelt som det gis?	Ja, informasjon om mulige konsekvenser av at samtykket trekkes, informeres om ved signering av samtykke
6.	Foreligger det informasjon til den registrerte om muligheten til å trekke tilbake samtykke?	Jmf pkt 5.
7.	Omfatter samtykket alle behandlinger og behandlingsformål som nevnt i DEL IV?	Nei, se pkt. 1 for nærmere utdyping.

- Gjennomgang av samtykke og vilkår for samtykke. Kontroller at samtykke ikke sammenblandes med kontrakt eller personvernerklæring.
- Gjennomgang av begrensninger eller mulighetsrom som samtykket gir. Beskriv hvordan den registrertes rettigheter ivaretas i vilkårene for samtykke.

III.3. Viderebehandling

[Dette punktet besvares kun dersom behandlingen er en viderebehandling av personopplysninger som tidligere er samlet inn for et formål.]

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Behandles opplysninger videre til andre formål enn opprinnelig formål (for eksempel forskning)?	Ja, til statistikk, anonymiserte opplysninger
2.	Dersom rettsgrunnlag for opprinnelig behandling av personopplysninger er lov eller forskrift, åpner lov eller forskrift for viderebehandling av personopplysninger?	Forskrift om rapportering fra kommuner og fylkeskommuner(kostraforskriften).
3.	Dersom opprinnelig behandling er basert på samtykke, dekker samtykket viderebehandlingen av de samme personopplysningene?	Personopplysninger viderebehandles ikke.

Nr.	Vurderingsspørsmål	Svar (forklar svar)
4.	Viderebehandles personopplysninger for statistiske formål?	Hvis ja, finnes det nødvendige garantier for å ivareta personvernet? Nevn garantier. NEI

III.4. Vurdering av formålet sett opp mot rettsgrunnlag

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Er formålet eller formålene klart definert?	Ja, jmf lovgivning
2.	Er formålet nedfelt i forskrift eller lov?	Ja, barnevernloven og forvaltningsloven, samt forskrifter
3.	Vil det være kontrollformål (for eksempel i annen lovgivning innenfor skatt, NAV, toll, politi, forsikring?)	Nei.
4.	Er det noe i egen forskrift eller andre forskrifter eller lover som begrenser formålet?	Nei. Kjenner ikke til slike begrensninger
5.	Er formålet beskrevet i løsning, tjeneste eller system utfordrende sett opp mot rettsgrunnlaget?	Ja Internkontroll, retningslinjer og rutinebeskrivelser
6.	Omfatter rettslig grunnlag både egne formål og utlevering?	Rettslig grunnlag omfatter eget formål
7.	Er formålet definert slik at det samsvarer med forventningene de registrerte kan ha ut fra egen forskrift, lov eller samtykkevilkår?	Ja. Den registrerte får begrunnelse og forklaring i kontakt med tjenesten.

III.5. Oppsummering

Her oppsummeres kort vurderingene som er gjort i DEL III.

DEL IV. Behandling av personopplysninger

IV.1. Oversikt over behandling og behandlingsaktiviteter

Nr.	Behandling	Detaljert beskrivelse av behandlingsaktiviteter
1.	Innsamling	Innhenting fra familiene selv, opplysningsinnhenting fra andre relevante offentlige tjenester. Fagsystemet er direkte koblet til folkeregisteret for registrering av personer.
2.	Lagring	Lagres i fagsystemet digitalt, til evig tid.
3.	Deling	Deles ikke, annet enn ved sak til rettsapparatet eller ved politisak. Nødvendig deling av personopplysninger ved henvisning til andre instanser
4.	Gi tilgang til	System admin og fagleder gir nødvendige tilganger til saksbehandlere
5.	Retting	Saksbehandler og leder på ulike nivå
6.	Sletting	Klientmapper slettes ikke. Ulike detaljer kan slettes eller endres av fagansvarlig. Dette er tilgangsstyrt ved angrefrister i systemet når det gjelder dokumenter.

IV.2. Systematisk beskrivelse og vurdering av behandling av personopplysninger

IV.2.1. Innsamling

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Hvilke typer personopplysninger samles inn?	Navn, adresse, personnummer, kontonr, mailadresse, personlige forhold, inntekt/økonomi ved behov, boforhold, helseopplysniger, etnisitet, opprinnelsesland, DUF nr. Seksuell legning i noen tilfeller

Nr.	Vurderingsspørsmål	Svar (forklar svar)
2.	Er noen av personopplysningene over kategorisert som særlige kategorier av personopplysninger? (for eksempel helseopplysninger, rase, fagforening osv.)	Ja.
3.	Hvordan samles personopplysningene inn?	Skriftlig. Direkte fra personen selv eller fra folkeregister.
4.	Samles personopplysningene inn direkte fra de registrerte selv eller fra andre kilder?	Se pkt over
5.	Er det noe som er særlig inngripende ved måten personopplysningene samles inn (for eksempel ved hjelp av fingeravtrykk, kamera- eller lydopptak, eller sporing av en persons lokasjon, biometri)?	Nei
6.	Samles det inn flere opplysninger enn det som er nødvendig ut fra formålet?	Nei
7.	Får den registrerte all informasjon som er påkrevd etter GDPR art.13 og 14?	Ja, nødvendig informasjon gis underveis i saken. Ellers på forespørsel om innsyn i egen sak.

IV.2.2. Lagring

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Hvordan skal opplysningene lagres?	Digitalt, på lokal server i kommunen.
2.	Hvor og hvor lenge lagres personopplysningene?	Se. pkt over. Til evig tid.
3.	Hvilke kriterier brukes for å bestemme lagringstid?	Lov om barneverntjenester
4.	Når skal personopplysningene slettes?	Skal ikke slettes
5.	Etter at formålet ved behandlingen er oppnådd, hvor lenge lagres personopplysningene før de slettes?	Slettes ikke.
6.	Er det utarbeidet rutiner for sletting?	Slettes ikke.
7.	Gis det informasjon til den registrerte om muligheten til å slette opplysninger og hvordan sletting kan gjøres?	Slettes ikke.

IV.2.3. Deling

Nr.	Vurderingsspørsmål		Svar (forklar svar)
1.	Utleveres eller tilgjengeliggjøres det personopplysninger til andre utenfor virksomheten?		Se IV. 1, pkt. 3. vedr deling.
2.	Hvordan utleveres eller tilgjengeliggjøres personopplysningene (dataflyt)?		Utveksles ikke via systemet. Lukket fagsystem i sikker sone.
3.	Er alle mottakere av personopplysninger identifisert og dokumentert (for eksempel ansatte, databehandlere, tredjeparter, eksterne virksomheter osv.)?		Visma er databehandler. Vi har ikke oversikt over underleverandører til Visma.
4.	a.	Hvordan deles personopplysningene mellom avdelinger internt i virksomheten?	Vi er kun en avdeling. Det er ikke fri informasjonsflyt. Informasjonen er tilgangsstyrt. Se arkivplan sikker sone.
	b.	Hvilke personopplysninger deles med hvilke avdelinger og hva er formålet med hver av disse delingene?	Tilgangsstyrt undersøkelse, tiltak og omsorg.
5.	a.	Hvilke eksterne virksomheter deles personopplysningene med (private, offentlige myndigheter osv)?	Ingen deling eksternt, ved unntak rettssystem og politi samt henvisninger til helse ved samtykke.
	b.	Hvilke personopplysninger deles eksternt, for hvilket formål og med hvilke rettslige grunnlag?	Relevante opplysninger Se pkt over.
6.	Vil personopplysningene overføres til andre land utenfor EU/EØS-området, og hva er det rettslige grunnlaget for overføringen?		Nei. Hvis ja, beskriv metode for overføring og land, samt risikovurderingen som er gjort.
7.	Vil personopplysninger overføres til tredjestater eller internasjonale organisasjoner (GDPR art.44-49)?		Nei

8.	Hvordan sikres etterlevelse av forordningen ved overføring til utlandet?	Overføres ikke
9	Finnes det annet regelverk, atferdsnormer/bransjenormer og retningslinjer som må følges?	nei

IV.2.4. Tilgang

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Hvem har tilgang til opplysninger?	Saksbehandlerne, fagansvarlig og sys.adm.
2.	Finnes det dokumentert rutiner for tilgangsstyring?	Ja, arkivplan sikker sone.
3.	Vil tilgangsstyringen for brukergruppene være rollebasert og tidsbegrenset?	Ja.
4.	Dersom det gis tilgang utenfor virksomheten, er det signert databehandleravtaler eller taushetserklæring?	Gis ikke.

IV.2.5. Retting

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Finnes det mulighet for retting av feil i den registrertes opplysninger?	Vi kan rette feil, slik som navn, adresse. Hvis det er skrevet feil og dokumentet er ferdigstilt, må vi legge inn en kommentar i nytt dokument og rette feilen. Den dokumentet omhandler kan også kommentere feil i dokumenter som blir registrert inn. Hvis feil dokument legges inn på feil person, kan dette dokumentet slettes.

2.	Gis det informasjon til den registrerte om muligheten til å rette opplysninger og om hvordan retting kan gjøres?	Ja, ved utsending av referat står det skriftlig at de kan kommentere referatet. Dette opplyses også i møtet.
3.	Finnes det dokumenterte rutiner for retting?	nei
4.	Dersom den registrerte ikke selv kan rette feil i egne personopplysninger, finnes det andre måter å gjøre det på?	De kan ikke selv rette personopplysninger, men de kan gjøre saksbehandler oppmerksom på feile personopplysninger. Saksbehandler retter feilen.

IV.2.6. Sletting

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Finnes det mulighet for sletting av den registrertes opplysninger?	nei
2.	Gis det informasjon til den registrerte om muligheten til å slette opplysninger og om hvordan sletting kan gjøres?	nei
3.	Finnes det dokumenterte rutiner for sletting?	nei
4.	Dersom den registrerte ikke selv kan slette egne personopplysninger, finnes det andre måter å gjøre det på?	nei
5.	Finnes det rettsgrunnlag i lov eller forskrift som gir grunnlag for å nekte sletting?	Arkivloven.

IV.3. Vurdering av sammenheng behandlingen utføres i (kontekst)

[I denne delen vurderes behandlingen i et større bilde. Alle interne og eksterne faktorer som kan påvirke forventninger eller konsekvenser vurderes her.]

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Vil det behandles personopplysninger fra ulike datasett, som er innsamlet for ulike formål og fra ulike behandlingsansvarlige?	Ja, i undersøkelser innhentes opplysninger for å kartlegge barnets/familiens

			situasjon. Opplysninger kan innhentes fra for eksempel PPT, BUP, sykehus, helsestasjon og politi.
2.	Hvilke kilder brukes for innhenting av personopplysninger?		Se punktet over.
3.	a.	Kobles systemene der opplysninger behandles opp mot andre informasjonssystemer?	nei
	b.	Finnes det tidligere erfaring med tilsvarende type behandling?	nei
4.	Finnes det noen nåværende tilfeller av allmenn bekymring for den beskrevne måten å behandle personopplysninger på?		nei
5.	Hvilken relasjon har den behandlingsansvarlige med de registrerte? Beskriv maktforholdet mellom dem.		Det er saksbehandler, som er habil i forhold til klienten. Saksbehandler vil ha en makt i forhold til den myndigheten som ligger til barneverntjenesten.
6.	Med tanke på at kompleksitet i den sammenheng behandlingen utføres i (kontekst), i hvilken grad har de registrerte kontroll over sine opplysninger?		De kan etter ønske få referater tilsendt, de blir informert om mulighet for å lese gjennom dokumenter og kontradiksjon. Opplysninger som innhentes gjennomgås med familien.
7.	Beskriv hvordan behandlingen vil oppfattes fra den registrertes synsvinkel. Kan for eksempel de registrerte oppfatte behandlingen som lite forutsigbar?		Det skal opprettes en plan for undersøkelsen som familien skal gjøres kjent med. Alle møter avtales med de enkelte i forkant, dette gjelder ikke uanmeldte tilsyn. Ved uanmeldte tilsyn vet

		vedkommende at dette er iverksatt. Noen av klientene kan oppleve saksbehandling som lite forutsigbart, da de er i en vanskelig livssituasjon og det kan være en ekstra belastning når barneverntjenesten kommer inn.
8.	Vil den registrerte ha en særskilt forventning om konfidensialitet (for eksempel dersom det omhandler helse, velferd, arbeidsforhold, kommunikasjon, lokasjon)?	Ja, de vil være opptatt av at opplysninger ikke blir spredd til noen som ikke har med saken å gjøre.

IV.4. Innebygd personvern

Nr.	Vurderingsspørsmål		Svar (forklar svar)
1.	Hvordan tenkes innebygd personvern og personvern som standardinnstilling ivaretatt i løsningen med tanke på:		
	a.	kravene til design?	
	b	sikker koding?	Dersom en saksbehandler skal inn i andres saker, må det dokumenteres hvorfor tilgang ønskes, før du får se det som er registrert av opplysninger.
	c.	testing og godkjenning før produksjonssetting?	Ja.
	d.	kontinuitets- og beredskapsplaner?	Det finnes undersøkelsesplaner, som er under innfasing.
	e.	jevnlige revisjoner?	Det er en ny løsning som er under produksjon. Det gjennomføres jevnlige

			oppdateringer av Visma Familia.
	f.	opplæring?	Det gis opplæring til nytilsatte. De som har jobbet lenger har gjennomgått opplæring med Visma. Det gis oppfriskning ved behov.
2.	Er alle prinsippene for behandling av personopplysninger ivaretatt i løsningen? – Se DEL V.1		Prinsippene for behandling av personopplysninger artikkel 5 blir fulgt.
3.	Hvordan er den registrertes rettigheter ivaretatt i løsningen? – Se DEL V.2 for hvilke rettigheter er det snakk om.		De har innsyn i registrerte opplysninger, har mulighet for kontradiksjon. Den registrertes rettigheter i kapitel 3 blir ivaretatt.
4.	Tas ny teknologi i bruk?		Ja. Regler for personvern bestrebes fulgt.
5.	Brukes eksisterende teknologi på en ny måte?		nei

IV.5. Ansvarsforhold

Nr.	Vurderingsspørsmål		Svar (forklar svar)
1.	a.	Er det noen avtale eller kontrakt med eksterne virksomheter om gjensidig forståelse for ansvar og roller?	Databehandler avtale med Visma
	b.	Gjenspeiler avtalen hvilke begrensninger som gjelder for behandling av personopplysningene?	ja
2.	a.	Brukes det databehandler?	ja
	b.	Er alle databehandlerne identifisert og er forholdet til dem avklart gjennom avtaler (GDPR art.28 nr.3)?	Ja, Visma.
3.	Om databehandleravtale:		
	a.	Gir databehandleren tilstrekkelige garantier for at egnede tekniske og organisatoriske tiltak som sikrer at behandlingen er i samsvar med forordningen (GDPR art.28 nr.1) vil gjennomføres?	ja

	b.	Er personvernprinsippene, for eksempel formålsbegrensning, dataminimering, lagring med videre ivaretatt i avtalen?	ja
	c.	Er de registrertes rettigheter og friheter ivaretatt i avtalen?	ja

IV.6. Vurdering av behandlingene samlet

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Vil planlagte behandlinger gjøre det lett eller vanskelig for den registrerte å utøve sine rettigheter?	Vet at de får en plan for fremgang i saken vil det være lettere for dem å utøve sine rettigheter.
2.	Vil planlagte behandlinger ut fra den registrertes synsvinkel preges av uforutsigbarhet eller lite åpenhet?	Ja, de vil kunne oppleve det som uforutsigbart og at barneverntjenesten er lite åpen. Men det etterstrebes at gjennomføringen skal være så forutsigbar og åpen som mulig.
3.	Er det usikkerhet knyttet til hvordan grunnleggende prinsipper for behandling av personopplysninger ivaretas (GDPR art.5)?	nei

IV.7. Oppsummering

Her oppsummeres kort vurderingene som er gjort i DEL IV.

Del V. Nødvendighet og forholdsmessighet av behandlingen

[Denne delen inneholder en vurdering av om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålene med behandlingen.]

V.1. Personvernprinsippene

Nr.	Vurderingsspørsmål		Svar (forklar svar)
1	Er behandlingen basert på lovlighet, rettferdighet og åpenhet (GDPR art.5.1 bokstav a og art.6 og 9)?		Ja.
	a.	Kommer det rettslige grunnlaget/behandlingsgrunnlaget tydelig frem?	Ja, det vises til lovhjemmel for åpning av sak. Det er også publisert personvernerklæringer på kommunens hjemmeside.
	b.	Vurder rimeligheten av behandlingen: Hva er forventede fordeler ved behandlingen? For virksomheten, den registrerte, samfunnet for øvrig osv.	Ja, det gjøres for å ivareta kommunens oppgaver etter Lov om barneverntjenester.
	c.	Hva vil konsekvensene være dersom behandlingene ikke gjennomføres?	Barn og familier kan oppleve å ikke få den hjelpen de trenger og har rett på.
	d.	Vurder hvordan åpenhet ivaretas i behandlingen.	Det vil etterstrebes åpenhet mot den det gjelder. Det vil alltid innhentes samtykk dersom det skal praktiseres større åpenhet mot andre.
2	Formålsbegrensninger		
	a.	Er formålet definert slik at det samsvarer med forventningene til de registrerte?	Ja.
	B	Har det vært vurdert andre alternativer for å oppnå formålet med behandlingen?	Nei, for å kunne utføre oppgavene til barneverntjenesten må informasjonen innhentes og lagres.
	c.	Finnes det mindre personverninngripende alternativer for å oppnå det samme formålet?	Nei.
	D	Vurder hvorvidt formålet kan oppnås med anonyme eller pseudonyme alternativer.	Det vil ikke kunne gi et bilde av den konkrete personens situasjon. Det vil kunne gjøre at

			rett hjelp ikke blir gitt på rett tid.
3	Dataminimering. Kan formålet oppnås ved for eksempel:		
	a.	å begrense innsamling av personopplysninger?	Nei, Det skal ikke innhentes opplysninger som barneverntjenesten ikke er i behov av.
	b.	med mindre detaljerte personopplysninger?	nei
	c.	uten fortrolige eller sensitive personopplysninger?	nei
	Begrunn nødvendighet og relevans relatert til formål for alle opplysninger som behandles.		Det er nødvendig og relevant for å kunne gi et bilde av den enkeltes situasjon slik at rett hjelp kan gis til rett tid.
4	Riktighet		
	a.	Vurder hvordan personopplysninger holdes korrekte og oppdaterte, med og uten den registrertes involvering.	Adresser kan sjekkes i folkeregistret, slik at dette kan oppdateres. Ved flyttinger passiviseres personen og flyttes til avsluttende saker. Det gjøres vurderinger om sak skal oversendes til ny kommune.
	b.	Vurder om det finnes nødvendig funksjonalitet for å rette og slette uriktige personopplysninger, ref. punkt IV.2.5 og IV.2.6.	Ja, dette er beskrevet tidligere.
	c.	Har dere rutiner som ivaretar kravet til korrekte og oppdaterte personopplysninger?	Ja, beskrevet tidligere.
5	Lagringsbegrensning		
	a.	Vurder om personopplysninger lagres etter at formålet er oppnådd og når opplysningene slettes.	Ja, de lagres i VSA til evig tid.
	b.	Vurder når personopplysninger anonymiseres eller pseudonymiseres som muliggjør videre lagring.	Nei de gjøres ikke anonyme.
	c.	Vurder hvilke garantier som må være plass dersom personopplysninger skal lagres i lenger perioder grunnet	Skal ikke benyttes til forskning og vil ikke

		arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål (GDPR art.89 nr.1).	være i allmenhetens interesse. Det rapporteres til Statsforvalteren og SSB anonymt om antall barn og i forhold til frist overskrider.
6.	Integritet og konfidensialitet – se DEL VI.1.		

V.2. Ivaretakelse av de registrertes rettigheter

Nr.	Vurderingstemaer	Vurdering
1.	Vurder hvordan informasjon til de registrerte gis (prinsippet om rettferdighet og åpenhet i behandlingen) (GDPR art.12, 13 og 14).	Det gis informasjon både skriftlig og muntlig. Informasjonen etterstrebes gitt på en åpen og lite krenkede måte til den som mottar informasjonen.
2.	Vurder hvordan den registrertes rett til innsyn ivaretas (GDPR art.15).	De kan få tilsendt dokumenter og de er informert om at de kan få lese dokumentene som omhandler dem, men ikke sensitive opplysninger som gjelder andre.
3.	Vurder hvordan den registrertes rett til retting og sletting ivaretas (GDPR art.16 og 17).	Klienten får informasjon om sin mulighet for kontradiksjon og at dette legges inn som dokument.
4.	Vurder hvordan den registrertes rett til innsigelser og begrensning av behandling ivaretas (GDPR art.18, 19 og 21).	Den enkelte kan ikke motsette seg en undersøkelse etter Lov om barneverntjenester.

		Det blir de også informert om skriftlig med henvisning til Lov.
5.	Vurder hvordan den registrertes rett til dataportabilitet ivaretas (GDPR art.20).	Ikke relevant
6.	Vurder hvordan forbud mot automatiserte individuelle avgjørelser, herunder profilering håndheves (GDPR art.22).	Ingen automatiserte avgjørelser. Vurderinger gjøres og vedtak fattes.

V.3. Ivaretakelse av de registrertes friheter

Nr.	Vurderingstemaer	Svar (forklar svar)
1.	Vurder hvordan de registrertes friheter i forhold til Den europeiske menneskerettskonvensjonen (EMK) er tatt hensyn til:	
	• Retten til privatliv og kommunikasjonsvern	Vurderer grunnlaget for å åpne undersøkelser.
	• Retten til ikke å bli diskriminert	Etterstreber å behandle alle med respekt. Ikke opptre dømmende
	• Tanke-, tros- og religionsfrihet	Etterstreber saksbehandling som ivaretar tanke, tros og religionsfrihet.
	• Ytrings-, og informasjonsfrihet	Etterstreber høy grad av ytringsfrihet. Være overbærende i forhold til klientens ytringer.

V.4. Oppsummering

Her oppsummeres kort vurderingene som er gjort i DEL V.

Del VI. Personvern risikoanalyse og planlagte tiltak

[Denne delen inneholder vurdering av risiko for de registrertes rettigheter og friheter, samt planlagte tiltak for å håndtere risikoene].

VI.1. Risiko, konsekvenser og sannsynlighet

VI.1.1. Sikkerhet ved behandlingen

[Fokuset i denne delen bør være sikkerhet i løsningen]

Nr.	Vurderingsspørsmål		Svar (forklar svar)
1.	Er personopplysningssikkerheten tilstrekkelig ivaretatt?		
	a.	Er det gjort en risikovurdering av løsningen (også ved endringer)? Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.	nei
	b.	Er det gjennomført tiltak for å håndtere risiko? Ved valg av tiltak skal det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter.	Ja, det er gjort grep i forhold til hvem som har tilgang til du ulike klientene. Leder kan gjennomgå hvem som har vært inne på ulike saker og hva som er årsaken til dette.
	c.	Er restrisiko håndterbar og akseptabel?	Ikke utført risikovurdering.
2.	Er alle iverksatte og planlagte tekniske og organisatoriske tiltak egnet til å sikre personopplysningenes konfidensialitet, integritet og tilgjengelighet?		Ja, dokumentert i sureway og utarbeidet arkivplan sikker sone.
3.	Beskriv hvilke forhåndsregler som tas for å beskytte personopplysninger (taushetserklæringer, databehandleravtale, atferdsnormer/bransjenormer, sikkerhetstiltak osv).		Alle som har tilgang til systemet har skrevet under taushetserklæring. Det er tilgangsstyring i familia for saksbehandlere. Det er inngått

		databehandleravtaler med Visma.

VI.1.2 Personopplysningsvernet

Nr.	Vurderingstemaer		Vurdering
1.	Med utgangspunkt i den registrertes perspektiv for hver risiko kan for eksempel følgende vurderes:		
	a.	Manglende reell medbestemmelse - den registrerte har ikke et valg, får ikke informasjon, får ikke innsyn, og så videre.	Den enkelte får ikke et valg om det åpnes undersøkelse, det etterstrebes at de skal få informasjon og innsyn i saken.
	b.	Manglende reell åpenhet - virksomheten evner ikke å forklare komplekse behandlinger eller forventet resultat ved sammenstilling av personopplysninger med andre datasett og så videre	Den enkelte kan oppleve mangel på åpenhet.
	c.	Manglende forutsigbarhet ved behandlingen - behandlingen er utenfor det den registrerte vil forvente og så videre.	Den enkelte kan oppleve mangel på forutsigbarhet.
2.	Hvilke konkrete rettigheter og friheter står i fare for å ikke innfris, jf. GDPR art.12-22 (rettigheter) og retten til privatliv, kommunikasjonsvern, ytringsfrihet, tanke-, tros- og religionsfrihet, retten til ikke å bli diskriminert og så videre (friheter)?		Ved at de ikke kan motsette seg en undersøkelse etter Lov om barneverntjenester kan de enkelte oppleve at deres rett til privatliv blir krenket. Ved at det er åpnet undersøkelse kan den enkelte føle seg diskriminert.

Generelt for vurdering av "Sikkerhet ved behandlingen" og "Personopplysningsvernet":

- Vurder risikoens opprinnelse, art, særegenhet og alvorlighetsgrad.
- Avklar potensielle **konsekvenser** for den registrertes personopplysningsvern for hvert risikoscenario.
- Anslå **alvorlighetsgrad** for hver risiko, særlig avhengig av hvilken inngripen en potensiell virkning har på den registrerte.

- Identifiser **trusler** og egenskaper ved løsningen som kan føre til hendelser og hvilke risikokilder som kan forårsake dem. Hvordan kan dette skje?
- Anslå **sannsynlighet** for at en hendelse oppstår, særlig ut fra en sårbarhetsvurdering og hva slags evne en risikokilde kan ha for å utnytte dem.

VI.2. Vurdering av planlagte tiltak

Nr.	Vurderingstemaer		Vurdering
1.	Beskriv tiltak for å håndtere risikoene for de registrertes og andre berørte personers rettigheter og berettigede interesser. Eksempler på tiltak kan være: - Garantier: krav til fornyet samtykke, rett til reservasjon osv. - Sikkerhetstiltak: tilgangskontroll, anonymisering, kryptering osv. - Mekanismer: funksjonalitet som er personvernfremmende for eksempel logging og sperring av tilgang eller sperring av informasjon		Systemet har tilgangskontroll slik at bare saksbehandler kommer inn, de andre må dokumenter hvorfor de er inne på saken. Fagansvarlig kan få oversikt over hvem som har vært inne i sakene og hvorfor.
2.	Ut fra tiltakene, vurder om:		
	a.	sikringen av vernet av personopplysninger er tilstrekkelig	Ja, kun leder og saksbehandler har tilgang på informasjon i saken.
	b.	de registrertes og andre berørte personers rettigheter og berettigede interesser er hensyntatt	Ja.
	c.	identifiserte risikoer er håndtert og akseptable	Ja, alle saksbehandler må dokumenter årsak til at de er inne på saker som omhandler noen de ikke er saksbehandler til. Alle saksbehandler skal logge ut av systemet og låse maskinen før de forlater den.
	d.	det er restrisiko etter alle planlagte tiltak	Det vil kunne være restrisiko, En annen

			saksbehandler kan få tilgang til en sak ved at den ansvarlige saksbehandler åpner saken for dem.

Kontroller om det er nødvendig eller mulig å forbedre hvert tiltak etter personvernregelverket og beste praksis innen sikkerhet. Hvis ikke, foreslå ytterligere tiltak og revurder nivået for hver risiko i lys av de nye tiltakene for å fastslå restrisiko.

VI.3. Oppsummering

Her oppsummeres kort vurderingene som er gjort i DEL VI.

Del VII. Involvering av personvernombudet

[I denne delen legges det opp til en vurdering fra personvernombudet. Personvernombudet involveres etter at DEL I – VI av denne malen er gjennomført.]

Vurdering fra personvernombudet

Del VIII. Ledelsens godkjenning og forhåndsdrøftelse med Datatilsynet

[I denne delen legges opp til en validering av DPIA av ledelsens gjennomgang, beslutning og godkjenning.]

Nr.	Vurderingstemaer	Vurdering
1.	Ledelsen vurderer hvorvidt de planlagte tiltakene, restrisikoen og handlingsplan er akseptable.	Tiltak og restrisiko er gjennomgått og det vurderes at handlingsplanen er akseptabel.
2.	Ledelsen beslutter og begrunner om DPIA er	DPIA er godkjent og behandling i

	○ Godkjent/validert: Behandling kan starte opp. ○ Betinget av forbedringer (forklar på hvilken måte): Revidert DPIA skal legges frem for ledelsen på nytt. ○ Avvist: Virksomheten beslutter ikke å gjennomføre behandlingen.	saksbehandlersystemet kan starte opp.

Dersom en DPIA har blitt behandlet i ledergruppen mer enn én gang, risikoen fremdeles er høy og viljen til å gjennomføre fremdeles er stor, må dere anmode Datatilsynet om forhåndsdrøftelse i tråd med GDPR art.36. Virksomheten må dokumentere at den ikke greier å gjøre risikoen lavere. Det er ledelsen som tar beslutningen om å anmode Datatilsynet om forhåndsdrøftelse.

*****

Lenke til Datatilsynets sjekkliste:
https://www.datatilsynet.no/globalassets/global/regelverk/veiledere/dpia-veileder/sjekkliste-for-dpiafaser.pdf

Lenke til uoffisiell norsk versjon av retningslinjer for vurdering av personvernkonsekvenser og beslutning om behandlingen kan "medføre en høy risiko" fra Artikkel 29-Arbeidsgruppen for beskyttelse av personopplysninger:
https://www.regjeringen.no/contentassets/1b6b0aebf624465f9704cadeaa320269/veileder_vurdering_personvernkonsekvenser_norsk_versjon.pdf