sopra steria

The world is how we shape it.

Direktoratet for eHelse

Høringssvar – Ny mal for DPIA

Sopra Steria

30. november 2021

Innholdsfortegnelse

1 Bakgrunn for våre innspill

Sopra Steria viser til Direktoratet for eHelses høring (21/699) på utkast til ny veileder «Mal for personvernkonsekvensvurderinger (DPIA) med veiledning til utfylling», med høringsfrist 30.11.2021.

Sopra Steria ønsker å takke Direktoratet for eHelse for arbeidet med oppdatering av DPIA-mal og veiledning. Vi har bistått flere virksomheter med slike personvernkonsekvensvurderinger, og det er et stort behov for gode maler og veiledning på personvernområdet, både i helsesektoren og i andre sektorer.

Sopra Steria er et ledende konsulentfirma innen digitalisering. Vi hjelper store private selskaper og offentlige virksomheter med å ta digitalt lederskap. Sopra Steria har i en årrekke hatt flere oppdrag innen informasjonssikkerhet og personvern for virksomheter i helsesektoren.

På bakgrunn av de erfaringene vi har gjort oss med virksomheter i helsesektorens tilnærminger til informasjonssikkerhet og personvern, mener Sopra Steria at vi kan komme med nyttige innspill til hvilken veiledning sektoren trenger på området for personvern. Konkret har vi hjulpet våre kunder med å gjennomføre flere DPIAer, og vi har innsikt i hvilke utfordringer helsesektoren møter i praksis når personvernkonsekvenser skal vurderes.

2 Tilbakemeldinger

Sopra Sterias tilbakemeldinger er strukturert etter de tre hovedspørsmålene som Direktoratet for eHelse spesielt ønsket tilbakemelding på:

1. Er dette en hensiktsmessig utforming av en mal for personvernkonsekvensvurdering til bruk i helse- og omsorgssektoren?
2. Dekker veiledningen til utfylling det meste av det virksomheten bør være oppmerksom på når den gjør en personvernkonsekvensvurdering?
3. Er formatet på produktet hensiktsmessig? (PDF med både mal og veiledning til utfylling, samt mal i word-format)

Delkapitlene vil være strukturert slik de er delt inn i malen, og henvisninger til malen og veilederen vil presiseres.

2.1 Er dette en hensiktsmessig utforming av en mal for personvernkonsekvensvurdering til bruk i helse- og omsorgssektoren?

2.1.1 Generelt for alle deler

Malen og veilederen inneholder flere henvisninger til eksterne veiledere, både fra EDPB, Artikkel 29-gruppen, og Datatilsynet. Sopra Steria mener det er mest hensiktsmessig at malen inneholder den veiledningen man mener er virktig for sektoren. Det er vår erfaring at særlig mindre aktører som i visse tilfeller mangler intern kompetanse på personvern, synes det er vanskelig å gjenfinne slike referanser. De kan også synes det er vanskelig å finne frem til det relevante innholdet når relevant dokument først er funnet. Vi antar at dette særlig vil kunne gjelde henvisningene til Artikkel 29-gruppen, ettersom organet er erstattet av EDPB, og det derfor vil kunne bli ekstra vanskelig å gjenfinne disse veilederne.

Videre ønsker vi at Direktoratet for eHelse presiserer hvor bindende denne malen er for helsesektoren. Vår erfaring er at mange dataansvarlige vil erstatte eget malverk med slike slike maler utarbeidet av myndighetene. Dersom Direktoratet for eHelse ser for seg at malen kan tilpasses de ulike virksomhetene, anbefaler vi at det tydeliggjøres.

2.1.2 Del A

Vi har ingen tilbakemeldinger på denne delen av malen.

2.1.3 Del B

Sopra Steria mener at del B bør inneholde en sjekkliste av hvilke momenter som som et minimum skal vurderes for å svare på om virksomheten trenger å gjennomføre en DPIA. Vi har lagt ved et eksempel på dette basert på Datatilsynets veiledning som vedlegg til dette høringssvaret som man kan ta utgangspunkt i. Dette kan være hensiksmessig da vurderingen av personvernkonsekvensvurderinger kan være vanskelig å forstå for flere.

Man kan i vurderingen av om det skal gjennomføres en DPIA også legge vekt på andre momenter enn de som kommer frem i Datatilsynets veiledning. Vi anbefaler at momenter som er spesielt viktige for helsesektoren presiseres i veilederen. Vi opplever også at flere virksomheter er usikre på hvordan de ulike momentene skal veies opp i mot hverandre, og vi anbefaler derfor Direktoratet for eHelse å tydeliggjøre hvilke kriterier som kan være utslagsgivende for når en DPIA skal gjennomføres.

I punkt 2.1 i malen, mangler det flere tekstmenyer som ikke er kommet med i utsendingen av utkastet for den nye DPIAen.

I punkt 2.2 i malen, kan virksomheten krysse av for at personvernombudet ikke har uttalt seg i vurderingen av behovet for å gjennomføre en personvernkonsekvensvurdering. Vi anbefaler at Direktoratet for eHelse inntar en ny del hvor virksomheten må begrunne hvorfor personvernombudet ikke har blitt involvert. Dette for å signalisere hvor viktig personvernombudets involvering er i en personvernkonsekvensvurdering. Dersom virksomheten etter at en DPIA er gjennomført kommer til at det er nødvendig å be Datatilsynet om en forhåndsdrøftelse, er personvernombudets kontaktinformasjon det første tilsynet ber om at skal oppgis. Videre vil tilsynet i slike prosesser ofte be om å kunne forholde seg til personvernombudet. Vi anbefaler at det derfor bør tydeliggjøres i malen at personvernombudets vurdering som hovedregel bør innhentes ved utarbeidelse av en DPIA.

2.1.4 Del C

Punkt 3.2 og 3.3 i malen bør inneholde en presisering om at virksomheten kan krysse av for flere kategorier av registrerte.

I punkt 3.6 i malen bør forskjellen på prinsippet lagringsbegrensing og den registrertes rett til sletting komme tydeligere frem. Malen bør forklare at retten til sletting er knyttet til at den registrerte selv kan be om sletting og at at dataansvarlig må kunne håndtere slike forespørsler, mens lagringsbegrensning er den dataansvarliges selvstendige plikt til å sørge for at personopplysninger ikke lagres lengre enn det som er nødvendig for å oppfylle formålet med behandlingen.

Sopra Steria anbefaler at punkt 3.6 og 3.9 i malen også synliggjør hvorvidt personopplysninger overføres til tredjeland. Dersom opplysningene overføres til tredjeland, anbefaler vi videre at malen også inneholder en mulighet for utfylling av Schrems II-vurderinger. Dette er vurderinger som vi ser at kundene våre trenger bistand til, og vi har god erfaring med å innta slike vurderinger i DPIAer.

Vi synes det videre er positivt at malen på en tydelig måte oppfordrer den som bruker den til å beskrive dataflyt i punkt 3.7.

Malen inneholder gode beskrivelser av om det foreligger et felles dataansvar med en annen virksomhet, og om det foreligger en databehandlerrelasjon. Vi mener det i tillegg kan være hensiktsmessig å beskrive hvorvidt behandlingen innebærer en overføring av personopplysninger til en annen dataansvarlig, for eksempel hvis en pasient blir henvist til behandling hos en annen dataansvarlig.

2.1.5 Del D

Vi anbefaler at overskriften i punkt 4.1 omformuleres til en mer aktiv formulering, for eksempel «Beskriv hvorfor man mener at vurderingen av personopplysninger er nødvendig for å ivareta formål». En annen mulighet er at man formulerer overskriftene i punkt 4.1 og 4.2 som spørsmål.

Vi har erfaring med at mange virksomheter har vanskeligheter med å følge opp tiltak som er identifisert i en DPIA. Vi anbefaler derfor at det inntas et punkt i malen som for eksempel viser en tiltakstabell hvor disse tiltakene er listet opp med frister og ansvarlige, både for gjennomføring av beslutninga av tiltak. I likhet med risiko, kan det være at visse tiltak må besluttes på et høyere ledelsesnivå, alt ettersom hva tiltaket inneholder. Det er vår erfaring at en slik tydeliggjøring vil gjøre det enklere for dataansvarlige å faktisk følge opp tiltak etter at en DPIA er gjennomført.

Del D i malen inneholder punkter fra 4.1 til 4.4, mens veilederen inneholder punkter fra 4.1 til 4.5. Punkt 4.4 i malen ser ut til å samsvare med punkt 4.5 i veilederen, mens punkt 4.4 i veilederen er tekst som ser ut til å tilhøre punkt 4.3 i malen.

2.1.6 Del E

Vi synes det er svært positivt at malen inneholder et eget punkt hvor den dataansvarlige kan dokumentere innspill som virksomheten har fått fra de registrerte. Det er vår erfaring at slike innspill gir dataansavarlig informasjon om mulig risikobilde ved behandlingen av personopplysninger. Slike innspill kan med andre ord være svært verdifull innsikt for en dataansvarlig. Vi anbefaler at man i tillegg inntar et punkt som tar for seg på hvilken måte den dataansvarlige har tatt hensyn til innspillene som er kommet fra de registrerte, eller deres representanter. Et slikt punkt kunne hatt som overskrift: «Hvordan har man tatt hensyn til innspillene som har kommet fra registrerte, representanter for de registrerte, og/eller andre interessenter?». Vi anbefaler også at punkt 5.1 i malen henviser til dokumentasjon på hvordan den registrertes mening er innhentet.

Det er vår erfaring at noen virksomheter i helsesektoren ikke har et veldig bevisst forhold til på hvilket ledelsesnivå en DPIA skal godkjennes. Vi anbefaler derfor at malen utformes på en måte som får den dataansvarlige til å tydeliggjøre hvem ledelsen er. Dette kan for eksempel gjøre ved å innta et punkt i malen med følgende overskrift: «Hvem er ledelsen i denne sammenhengen?».

Restrisikonivået i en DPIA vil påvirke på hvilket ledelsesnivå i virksomheten som skal beslutte DPIAen. Vi anbefaler derfor at Direktoratet for eHelse synliggjør dette, enten i malen eller i veiledningen. Dette kan for eksempel gjøres ved å innta en beskrivelse av hvilket ledelsesnivå som skal godkjenne DPIAen på de forskjellige nivåene av restrisiko (høy, middels, lav) i punkt 5.3 i malen.

2.2 Dekker veiledningen til utfylling det meste av det virksomheten bør være oppmerksom på når den gjør en personvernkonsekvensvurdering?

2.2.1 Generelt for alle deler av veilederen

Generelt synes Sopra Steria at veilederen er god. Den inneholder flere gode eksempler på hvordan malen kan utfylles. Vi synes at man nesten aldri kan ha for mange eksempler. Eksempler gjør det langt enklere for en uerfaren dataansvarlig å kunne bedre forstå gjennomførelsen av personkonsekvensvurderingen. Vi anbefaler

derfor at Direktoratet for eHelse inntar enda flere gode eksempler i veilederen. Dette gjelder spesielt der det ikke allerede inngår eksempler.

2.2.2 Del A

Vi opplever noen ganger at spesielt helsesektoren har svært komplekse ansvarsforhold mellom virksomheter. Det er derfor ikke alltid lett å identifisere hvem som er dataansvarlig. Direktoratet for eHelse kan derfor vurdere å komme med eksempler på dataansvarlige virksomheter i veilederen punkt 1.1.

Vi anbefaler at Direktoratet for eHelse kommer med eksempler på prosjektnavn, prosesser eller løsninger som kan være aktuelle i punkt 1.3.

Det er vår erfaring det kan være hensiktsmessig å definere hvilket ledelsesnivå som skal godkjenne en DPIA tidlig i prosessen. Vi anbefaler derfor at Direktoratet for eHelse spesifiserer at det er dataansvarlig som skal godkjenne behandlingen som skal gjennomføres i punkt 1.5. Vi anbefaler også at direktoratet presiserer at listen med aktuelle deltakere/roller ikke er uttømmende.

Vi synes eksemplene som Direktoratet for eHelse fremhever for å illustrere hvordan et personvernombud kan involveres i en DPIA, er svært gode.

2.2.3 Del B

Del B Punkt 2.1 i veiledningen inneholder flere henvisninger til eksterne kilder som det oppfordres til at de som bruker veilederen, tar en nærmere titt på. Som tidligere nevnt, refereres det til en veiledning fra artikkel 29-gruppen, som er erstattet med EDPB. Det kan være vanskelig å gjenfinne denne veiledningen uten referanse til EDPB.

Veilederen punkt 2.1 gjengir en illustrasjon fra daværende artikkel 29-gruppes (nå EDPBs) veiledning om når en DPIA skal gjennomføres. Vi synes at denne figuren kan være noe vanskelig å forstå, og vi anbefaler at det i stedet utarbeides en illustrasjon med spørsmål som guider de dataansvarlige til neste steg som skal vurderes. Figuren ville da kunne fungert som en sjekkliste for å se om personvernkonsekvensvurderinger må gjennomføres.

Videre anbefaler vi at Direktoratet for eHelse inntar en forklaring på hvorfor man gjennomfører DPIA i veilederens punkt 2.2. En slik forklaring bør også inneholde litt om hvilken kompetanse man må ha for å gjøre en DPIA. Etter vår erfaring, er det ikke alle virksomheter som har etablert et personvernombud. Dette gjelder særlig mindre virksomheter, og det kan derfor også være hensiktsmessig å forklare hva en virksomhet skal gjøre dersom man ikke har et etablert personvernombud. Vi anbefaler videre å innta eksempler på gode og dårlige vurderinger som kan brukes til inspirasjon og læring.

I setningen «På bakgrunn av punktene over tar virksomheten stilling…» i punkt 2.3, kan være noe forvirrende om man refererer til alle punkter over fra både del A og B eller bare del B. Vi anbefaler derfor at det spesifiserer nærmere hva som inngår i punktene over.

Vi anbefaler at det presiseres i punkt 2.4 i veilederen at relevante fagpersoner bør involveres i denne prosessen. Det kan være hensiktsmessig å henvise direkte til forordningen som sier noe om advokatkompetanse.

Etter vår erfaring trenger dataansvarlige ofte bistand til å forstå hvilken type dokumentasjon som er tilstrekkelig for å demonstrere etterlevelse til personvernforordningen. For å hjelpe dataansvarlige i helsesektoren med å forstå hvordan etterlevelse kan dokumenteres, anbefaler vi derfor at Direktoratet for eHelse kommer med eksempler også for punkt 2.2 til 2.4.

2.2.4 Del C

En og samme behandling av personopplysninger kan ha flere formål. Behandling av personopplysninger i en pasientjournal kan for eksempel både ha som formål å skulle bidra til forsvarlig helsehjelp, oppfylle helsepersonells dokumentasjonsplikt, bedre pasientsikkerheten, oppfylle krav til rapportering til offentlige myndigheter, tilsyn og kvalitetskontroll. I punkt 3.1 legges det til grunn at man bare har ett formål, og vi anbefaler at veiledningen beskriver hvordan en behandling kan ha flere formål.

Dersom man har flere formål, kan også disse ha ulike slettetidspunkt. Det kan være at en dataansvarlig også ønsker å begrense tilgangen til noen over tid og da vil også dette tidspunktet ikke være statisk. I punkt 3.1 anbefaler vi derfor at det også inntas en kort beskrivelse av hva formål er, da det ikke er gitt at alle dataansvarlige er klar over hva et formål er. Vi anbefaler at dette også illustreres med eksempler på gode formålsbeskrivelser.

Av hensyn til mindre dataansvarlige som ikke tidligere har mye erfaring med gjennomføring av DPIAer, anbefaler vi at det i veilederen for «Rettslig behandlingsgrunnlag» defineres hva som menes med behandlingsgrunnlag, eksempelvis i definisjonskapittelet.

Vi anbefaler å eksemplifisere punkt 3.3 i veilederen ytterligere med personer med nedsatte kognitive evner, samt personer som er umyndiggjorte. Vi tror det også kan være hensiktsmessig å presisere at pasienter og pårørende inngår som sårbar gruppe. Vi mener at beskrivelsene av skjevheter i maktforhold for registrerte som ikke har samtykkekompetanse bør flyttes fra punkt 3.4 til punkt 3.3, og skjevheter i maktforhold kan kobles til vurderingen av hvem som faller inn under begrepet «sårbar gruppe».

Som tidligere nevnt synes vi det er positivt at malen legger opp til at den dataansvarlige skal beskrive dataflyt. Vi har god erfaring med bruk av flytdiagram for å beskrive dataflyt. Vår erfaring er at en illustrasjon gjør det enklere for den dataansvarlige å beskrive hvordan personopplysninger skal behandles. Dette kan for eksempel gjøres ved å lage et flytdiagram over hvor personopplysninger behandles i det enkelte informasjonssystemet, eller det kan illustreres ved beskrivelse av hvordan personopplysninger behandles i virksomhetens prosesser. Vi anbefaler derfor Direktoratet for eHelse å fremheve gode eksempler på dette i veiledningen. For pseudonymiserte eksempler fra Sopra Steria, se vedlegg 2. Det kan også være en idé å komme med eksempler i formatet til de verktøyene som virksomheter kan bruke, for eksempel Power Point eller Miro.

Vi synes stikkordene som blir oppgitt i punkt 3.8 i veilederen er svært gode og forklarende.

Under punkt 3.9 i veilederen foreslår Sopra Steria at Direktoratet for eHelse tydelig oppfordrer til at avtaler bør legges ved. Istedenfor å "*beskrive avtalen*", kan det være hensiktsmessig å heller be de dataansvarlige"*fortell konkret hva databehandleren gjør hos dem/for dem*". Vår erfaring er at en beskrivelse for bruk av leverandør vil si veldig lite for dataansvarlige som ikke har mye erfaring på personvernområdet.

Vi synes punkt 3.12 i veilederen er godt skrevet og inneholder et fint og nyttig eksempel.

Vi erfarer at mange dataansvarlige i helsesektoren har utfordringer med å bygge personvern inn i sine løsninger. Innebygd personvern settes ofte bort til leverandøren som skal utvikle systemet, uten at dataansvarlig stiller krav og bekriver hvilke personvernrettigheter som skal bygges inn i løsningen. Det finnes en rekke spesifikke personvernrettigheter i helsesektoren, for eksempel vergeinnsynsreservasjon, retten til innsyn i oppslag i egen pasientjournal, retten til sperring, og til en viss grad vil også helsepersonells taushetsplikt være en personvernmekanisme som må bygges inn i informasjonssystemer. Dette er eksempler på spesielle rettigheter som dataansvarlige bør være klar over skal bygges inn i løsninger som anskaffes i helsesektoren. Det vil ofte ikke være nok for dataansvarlige å overlate innebygd personvern til en leverandør, de dataansvarlige må definere hva innebygd personvern konkret betyr. Vår erfaring er at dataansvarlige bør være så tydelige som mulig, hvis ikke blir denne oppgaven raskt outsourcet til underleverandør som ikke nødvendigvis klarer å bygge inn personvernmekanismer generelt, og i alle fall ikke helsesektorens spesifikke personvernmekanismer. Vi anbefaler derfor at Direktoratet for eHelse tydeliggjør dette i veiledningens punkt 3.13.

I tillegg, mener vi det er behov for en hjelpetekst som beskriver hva innebygget personvern er i punkt 3.13, og hvordan personvern kan bygges inn i løsninger. Dette bør eksemplifiseres, slik at det er lett for virksomheter med ulik modenhetsgrad og kompetanse på personvern å forstå hva innebygget personvern innebærer.

Vi ber Direktoratet for eHelse vurdere om det er hensiktsmessig å lage en begrepsliste i veiledningen.

2.2.5 Del D

Vi synes det er positivt at det benyttes spørsmål i punkt 4.2 for å hjelpe virksomheten med å svare ut om hvorfor det ikke vil være mulig å ivareta formålene på en mindre inngripende måte. Vi ber Direktoratet for eHelse vurdere om spørsmålene kan omformuleres ved å snu på ordlyden fra «Hvorfor ikke..?» til «Er det mulig å..?». For eksempel endre «Hvorfor er det ikke tilstrekkelig å behandle personopplysninger om et mindre antall personer?» til «Er det tilstrekkelig å behandle personopplysninger om et mindre antall personer?».

En god del av de dataansvarlige i helsesektoren har allerede egne kontrollsystemer på plass. Det kan derfor være hensiktsmessig at punkt 4.3 i veilederen åpner opp for at de tiltakene som identifiseres skal følges opp i linjen som en del av de dataansvarliges egne internkontrollsystem. Dette vil kunne føre til en bedre oppfølging av tiltak. Skjemaet som blir brukt i malen i dag kan være et eksempel og et utgangspunkt, men vi mener det kan være hensiktsmessig å spesifisere i veilederen at tilpasninger kan gjøres ut i fra eget kontrollrammeverk.

I del D punkt 4.4 i veilederen for tabellen «Eksempler på utfylling» er det en feil i den øveste cellen i tabellen. Det vises en celle hvor teksten kuttes halvveis i setningen «Store mengder helseopplysninger og personopplysninger av svært personlig karakter behandles». Ellers i punkt 4.4 i veilederen synes vi det brukes gode eksempler og dersom det finnes flere, oppfordrer vi til å innta disse også. Vi oppfordrer også Direktoratet for eHelse til å innta flere eksempler i listen «Eksempler på mulige konsekvenser som kan følge». Her kan det for eksempel nevnes

konsekvenser knyttet til diagnose som konsekvenser for foresatte av barn eller misinformert redsel knyttet til en misforstått diagnosen som kan få konsekvenser for pasientens evne til inntekt. For konsekvensen «Risiko for skade på omdømme for den registrerte» kan det også nevnes hvilken subjektiv belastning det kan få for den enkelte hvis deres personopplysninger kommer på avveie. Dette vil da være noe som utfordrer den registrertes tillit til dataansvarlig som helsetjeneste og vil mulig medføre ubehag for den registrerte.

Vi mener generelt at del D i veilederen bør inneholde en overordnet konkretisering av hva Direktoratet for eHelse er ute etter på risikovurderingen. Det kan her også henvises til at den dataansvarlige selv kan ha en internmetode for risikostyring som også inkluderer personvern. Vår erfaring tilsier at det kan være utfordrende å vurdere personvernkonsekvenser, og det ikke er sikkert at den klassiske risikofremgangsmåten er like hensiktsmessig for helsesektoren. For å hjelpe mindre virksomheter som har lite erfaring med risikovurderinger, anbefaler vi at veiledningen sier noe mer om hvordan man kan vurdere risiko, herunder mer konkret informasjon om risiko, sannsynlighet og konsekvens. Dette kan være med på å hjelpe dataansvarlige i helsesektoren å få en bedre felles forståelse for hvordan vurdere risiko.

2.2.6 Del E

Vi ser at mange aktører spesielt i helsesektoren inngår i komplekse forhold med hverandre, og det kan være uklart hvem som er dataansvarlig og databehandler. Vi opplever også at databehandlere i utgangspunktet har mer kunnskap om informasjonssikkerhet og personvern enn dataansvarlige, og derfor i stor grad vil sette premissene for behandlingen av personopplysninger. Vi anbefaler derfor at Direktoratet for eHelse i tillegg til registrerte, respresentanter for de registrerte og/eller andre interessenter også kommer med en klar oppfordring til at innspill også bør hentes fra dataanasvarlige og databehandlere i veilederens punkt 5.1. Disse innspillene er noe som bør innhentes tidlig og gjerne før risikovurderingen. Det kan gjerne fremgå eksempler her som beskriver hva man har tenkt å gjøre i behandlingen.

Vi synes veilederen retter søkelyset mot den registrertes forventninger på en god måte i del E. Vår erfaring er at innspill fra den registrerte også kan komme gjennom andre kanaler, for eksempel brukertester, og det kan være verdt å nevne dette i veiledningen.

Vi ser på det som positivt at veilederen i punkt 5.3 legger opp til at ledelsen kan begrunne sin vurdering skriftlig. Vi anbefaler at man i tillegg beskrivelser hvem ledelsen kan være, og at personvernrisiko kan måtte aksepteres av ulike ledernivåer og instanser ut i fra hvilken vikrsomhet man tilhører, og hvilken restrisiko man har etter at DPIAen er gjennomført. Vi anbefaler videre at dette punktet inneholder en oppfordring til å å løfte høy gjenværende personvernrisiko til et høyt nivå i ledelsen. Vår erfaring er at det kan det være lurt å avklare på forhånd hvilket risikonivå man skal legge seg på og hvem som tar avgjørelsen om restrisiko på de forskjellige nivåene. Vi anbefaler derfor at Direktoratet for eHelse inntar en veiledning på hvordan man gjennomfører vurdering av riskoen og hvordan en skal komme til et resultat i veilederen punkt 5.3.

2.3 Er formatet på produktet hensiktsmessig? (PDF med både mal og veiledning til utfylling, samt mal i word-format)

Vi har erfaring med utforming av DPIA i flere formater og i flere medium, for eksempel Word, Excel, Confluence og Jira. Vi mener at mest verdiskapende måten å tilnærme seg en DPIA på, er å starte vurderingen tidlig i en anskaffelses- eller utviklingsprosess. Dette fordi de risikoer som man som dataansvarlig identifiserer gjennom DPIAen, dermed vil kunne få en direkte påvirkning for designvalg i den endelige løsningen. For å best svare på dette behovet, mener vi at bruk av løsninger som Confluence kan være hensiktsmessig. Større virksomheter som NAV, har i flere år brukt maler i Confluence for å løse dette behovet. Vi anbefaler derfor at Direktoratet for eHelses mal for DPIA, også tilgjengliggjøres i slike format.

3 Vedlegg

1. Sjekkliste for pre-DPIA
2. Eksempler på flytdiagram for data i Power Point