



«Informasjonssikkerhet og personvern – gjennomføring av DPIA for digitalt tilsyn».

Prosess og erfaring fra Lindesnes



- Presentasjon av prosess og arbeid utført i Lindesnes, Mandal & Marnardal (Nye Lindesnes)
- Erfaringer og innspill til arbeid med DPIA
- Samarbeid med Normen og Agderprosjektet
- Ingen svar med to streker under!



Forløp/prosessen



Veileder fra
Datatilsynet

Sjekkliste fra
Datatilsynet

Behandlingsprotokoll

Mal for DPIA

Mal for
Ros analyse



Veileder – fra Datatilsynet



- Veileder for vurdering av om personvernkonsekvenser (DPIA) skal gjennomføres
- Går igjennom regelverket



Digitalt tilsyn - Axis videokamera



- Tilsyn via kamera (erstatte fysisk tilsyn)
- HD kamera med IR lys for videovisning i mørket
- Sikker pålogging med ID porten
- Kan ta stillbilde og streame video (se live video)
- Innbygd mikrofon for kunne høre lyd
- All overføring av data (bilde eller kamera) er kryptert



Risiko informasjonssikkerhet



• Ros analyse og Tiltakskort

[Lindesnes ros analyse digitalt tilsyn.doc](#)

RISIKO- OG KONTROLLMATRISE

Lindesnes kommune

Bakgrunn for analysen: (Hvorfor lages analysen?)	Digitalt tilsyn
Deltakere i analysen:	Kjell Ivar Syvertsen, Anita Grødem Borhaug og Marianne Mønsås
Dato gjennomført:	01.11.18

Sannsynlighet	Verdi	Eksempel
Lite sannsynlig	1	En gang pr 100 år
Mindre sannsynlig	2	
Sannsynlig	3	En gang pr 5-10 år
Meget sannsynlig	4	
Svært sannsynlig	5	Når som helst

Konsekvens	Verdi	Eksempel
Lav	1	Ingen personskade
Moderat	2	Mindre personskade
Høy	3	Alvorlig personskade
Kritisk	4	Flere alvorlig skadd
Katastrofal	5	Dødsfall/mange skadd

Se veiledning i tabell øverst til høyre, og gi poeng 1-5. Multipliser poeng, og sett kryss. Hvis risikoen er høyere enn 20 bør det iverksettes tiltak.

ID	1. Hva kan gå galt	2. Hvor galt kan det gå?					3. Hva er gjort for å unngå at det går galt?	4. Er det nok?	5. Oppfølging		
Nr	Identifisert risiko / trussel / uønsket hendelse	Beskriv kort hvilke konsekvenser som kan inntreffe.	Sannsynlighet	Konsekvens	Lav <9	Høy >10	Etablerte tiltak for å redusere risiko	Gjenværende risiko etter tiltak	Hva	Ansvarlig	Frist
1.	Får ikke logget seg på server til Telenor - Server nede - Ruter nede - Strømmen borte	- Får ikke sett på kameraet til brukere. - Må reise ut til vedkommene	4	2	8		- Server levert ifra Telenor. Kjenner ikke påliteligheten til denne. Kan ikke gjøre noe med denne. - Rutiner/prosedyre for å legge inn nye ansatte i tjenesteforløpet	ja			
2.	Får ikke logget seg inn i plattformen: - Glemte telefonen med bankID/passord - Har ikke lagt inn nyansatt	- Får ikke sett på kameraet til brukere. - Få annen ansatt på jobb som kan logge seg inn	4	2	8		- Flere ansatte med tilgang pr vakt				

23.10.19

Farge:	Beskrivelse:	Tiltak:
Grønn	Kamera fungerer slik det skal	Rutine ved innlogging av ansatte - Logg deg inn på følgende web side: https://www.smarttracker.no/digtil/#login - Se prosedyre og brukerveiledning på Ikks
Gul	Feil ved et kamera	Oppdages feil på kamera har tjenesten ansvar for å: - Dagtid kan hjelpemiddelkoordinator kontaktes pr telefon - Ellers melde til lin.hjelp.profil@lindesnes.kommune.no - Dersom feilen ikke kan utbedres må der utføres tilsyn iht tiltak i pasientjournal. Hjelpemiddelkoordinator - Responstid vil normal være i løpet av 24 timer på ukedager - Tilbakemelding vedr status på kamera gis til daglig leder - Ved varslet nedetid må daglig leder ha beskjed
Rød	Ved feil på flere kamera	Varsler om systemfeil kan komme fra ulike aktører (Telenor, Agder energi, ansatte) - Ved varslet nedetid må daglig leder ha beskjed - Dagtid kan hjelpemiddelkoordinator Kjell Ivar Syvertsen kontaktes på tlf: 382 55204/913 75 896 - Ellers melde til lin.hjelp.profil@lindesnes.kommune.no - Tjenesten må gjennomgå alle som har kamera, og iverksette tiltak ut fra individuelle avtaler som er gjort med bruker og pårørende. - Ved behov må der kalles inn ekstra bemanning - Prioriteringer skal sikre at de mest pleietrengende får nødvendig helsehjelp. Blir feilen ikke rettet innen rimelig tid må tjenesten: - avklare brukes kognitive tilstand - avklare muligheten for pårørende som en ressurs - avklare behovet for ekstra tilsyn - avklare behov for å ekstra bemanning i hjemmet - evt tilby bruker plass inne på avdelingen (gjelder for hjemmeboende)

Hvem skal delta ved gjennomføring av DPIA?



- Behandlingsansvarlig er ansvarlig for at DPIA gjennomføres
- **Deltagere**
 - Personvernombud
 - Databehandler
 - De registrerte eller deres representant
 - Uavhengige eksperter (it, ikt..)
 - Informasjonssikkerhetsansvarlig



Arbeidsgruppe Nye Lindesnes



- Marianne Holmesland Lindesnes - Velferdsteknologi koordinator
- Anne Lans Syvertsen Lindesnes - Informasjonssikkerhetsansvarlig
- Janne M Heddeland Mandal– Informasjonssikkerhetsansvarlig
- Stian Broberg Mandal - Velferdsteknologi koordinator
- Tone Hinna Hovednak Nye Lindesnes – Prosjektkoordinator
- Gudrun Røssehaug Marnardal - Informasjonssikkerhetsansvarlig
- Adele Aanonsen Marnardal – kontaktperson velferdsteknologi
- Guro Gidske DDV – personvernombud
- Marit Svindland Agderprosjekt – prosjektleder
- Helge Pedersen Brukerrepresentant



DEL I. Vurdering av behov for DPIA



Nr.	Vurderingsspmå	Ja/Nei
1.	Er dette et nytt prosjekt eller prosess?	Ja
2.	Vil prosjektet innebære innsamling av ny informasjon om enkeltpersoner?	Nei
3.	Vil prosjektet be enkeltpersoner om å gi informasjon om seg selv?	Nei
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)?	Nei
6.	Innebærer prosjektet at du bruker ny teknologi som kan oppfattes som inngripende for personvernet? For eksempel, bruk av biometri eller ansiktsgjenkjenning?	Ja
7.	Vil prosjektet resultere i at du tar beslutninger eller gjennomfører tiltak mot enkeltpersoner på måter som kan ha en betydelig innvirkning på dem?	Nei
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, kan det bety at det er behov for DPIA.

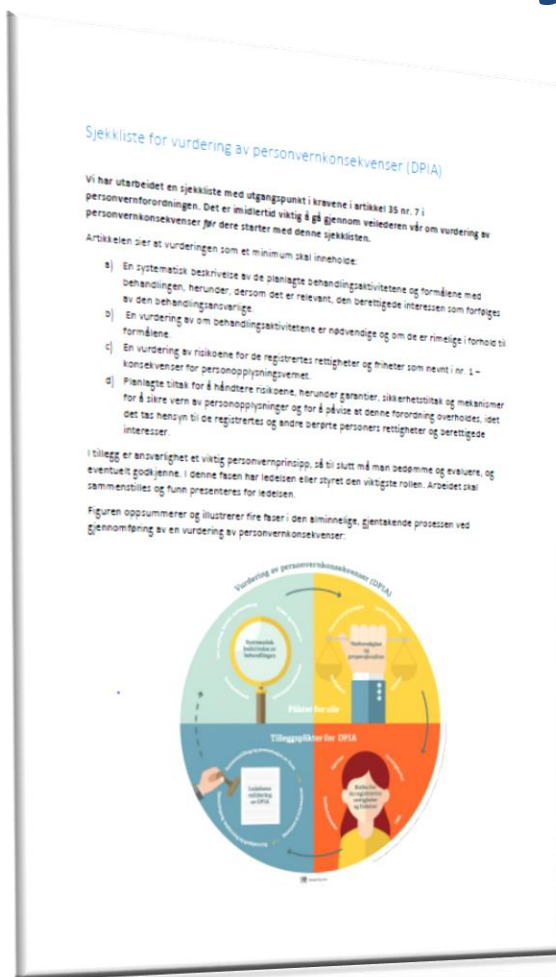
Forsett videre



Sjekkliste – fra Datatilsynet



- Utgangspunkt i kravene i artikkel 35 nr. 7 i personvernforordningen
- Hva må man tenke på?
- Figuren oppsummerer og illustrerer fire faser i den alminnelige, gjentakende prosessen ved gjennomføring av en vurdering



[Datatilsynet sjekkliste](#)



DPIA mal



 Direktoratet for e-helse

[Versjonsnr.1.0/25.5.18]

[DPIA mal](#)

Mal for 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.



Forløp/prosess



Veileder fra
Datatilsynet

Sjekkliste fra
Datatilsynet

Behandlingsprotokoll

Mal for DPIA

Mal for
Ros analyse



Fase 1



Kvalitetssjekker at det er en fullstendig oversikt over behandlingen, og at beskrivelsen av den er komplett og tydelig.

Systematisk beskrivelse av behandlingen

- Art, omfang, formål, sammenheng
- Kilder og mottagere
- Informasjonssikkerhet
- Ansvarsforhold



Behandlingens art



Forsikre deg om at beskrivelsen omhandler behandlingens iboende karakteristikk.

- Er det en behandling som gjør det lett eller vanskelig for de registrerte å utøve sine rettigheter?
- Er det en behandling som fra den registrertes synsvinkel preges av uforutsigbarhet og lite åpenhet?
- Er det usikkerhet knyttet til hvordan grunnleggende prinsipper for behandling av personopplysninger ivaretas, jf. artikkel 5?

«Systematisk behandling av personopplysninger»

Behandlingen

- skjer i henhold til et system
- er forhånds arrangert (planlagt) organisatorisk eller metodisk
- skjer som følge av en plan om å samle inn personopplysninger
- skjer som en del av en strategi





Henvising og kartlegging

Ny bruker:

1. Søknad/henvendelse om tjeneste fra kommunen
2. Saksbehandler vurderer/kartlegger om bruker/pårørende vil ha nytte av digitalt tilsyn.
3. Saksbehandler fatter vedtak og tildeler tjenesten i Profil. Vurderer/innhenter opplysninger om samtykkekompetanse,
4. Utføre en gevinstkartlegging (nullpunkts måling) ved hjelp av sjekklister.
5. Saksbehandler oversender løpenummer og vedtaksdato per mail til hjelpemiddelkoordinator og hjemmetjenesten. Nødvendig informasjon skrives inn som rapport under plankategorien hjelpemidler; området velferdsteknologi; tiltaket ny bruker.
6. Foreta en detaljkartlegging, tilpasset personlige innstillinger, bruk avtale skjema

Revurdering:

1. Tjenesten/gruppeledere vurderer om bruker kan ha nytte av digitalt tilsyn. Sender revurdering til saksbehandler.



Tilpasning og installasjon

1. Velferdsteknologi koordinator bestiller kamera og simkort ved behov utfra bestillingsskjema.
2. Ved nyansatte: daglig leder sender tilgang skjema og gir hjelpemiddelkoordinator beskjed om personnummer til nye ansatte som skal ha tilgang til kameraer i Lindesnes
3. Hjelpemiddelkoordinator mottar epost. Foretar nødvendige bruker registrering i Web løsningen utfra rapport i profil
4. Hjelpemiddelkoordinator kontakter bruker og pårørende og avtaler tidspunkt for montering/opplæring. Tilpasse innstillinger for digitalt tilsyn til bruker. Gir beskjed til hjemmetjenesten.
5. Hjemmetjenesten gjør seg kjent med vedtak og foretar nødvendig registrering i Profil.
6. Hjemmetjenesten lager tiltak i profil for:
 - Tidsintervaller for digitalt tilsyn (etter egen avtale)
 - hvis det ikke fungerer (Ros)



Opplæring

1. Nødvendig opplæring og tilgang til ansatte blir gitt.
2. Bruker og evt pårørende får muntlig informasjon om kamera, utdeling av informasjonsskriv samtidig som monteringer skjer av hjelpemiddelkoordinator
3. Testperiode over to uker hvor tjenesten følger opp tett. Hvordan håndterer bruker/pårørende digitalt tilsyn, bør innstillingene endres osv. Dokumenteres i profil
4. Prosedyrer og rutiner og opplæringsmanual knyttet opp mot digitalt tilsyn ligger på kommunens intranett side.



Daglig drift

1. Digitalt tilsyn utføres med å logge på web løsning; <https://www.smarttracker.no/digitalt/#/login> etter avtalt intervall med bruker/pårørende, hjemmetjenesten må respondere på behov for hjelp/hendelser
2. Dokumentere hendelser/avvik i Profil. Ved feil melde inn til: lin.hjelp.profil@lindesnes.kommune.no
3. Følge opp gevinster, etter kommunens rutiner.



Evaluering

1. Vurdere hvilke effekter digitalt tilsyn har for bruker, pårørende og ansatte.
2. Evaluere etter behov:
 - Revurderer tjenesten
 - Evaluere hvordan bruker/pårørende og tjenesten opplever digitalt tilsyn.
 - Evaluere om innstillinger bør endres. Ved endring skriv inn som rapport under plankategori hjelpemidler- område hjelpemidler- tiltak ny/endre bruker. Send mail med løpenummer til lin.hjelp.profil@lindesnes.kommune.no
3. Registrere nye data for gevinstrealisering(eks. vedtakstimer eller redusert antall tilsyn)
4. Dokumentasjon i profil

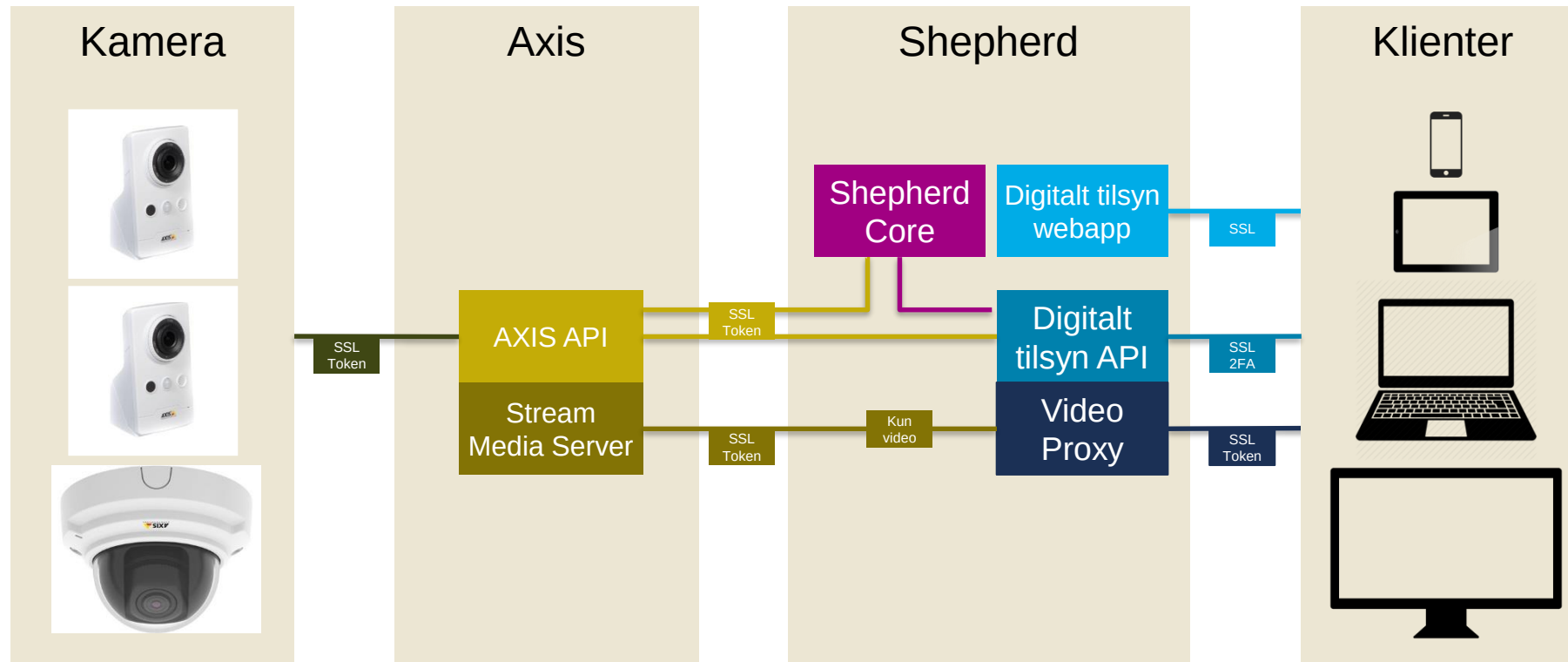


Videreføre/ avslutte

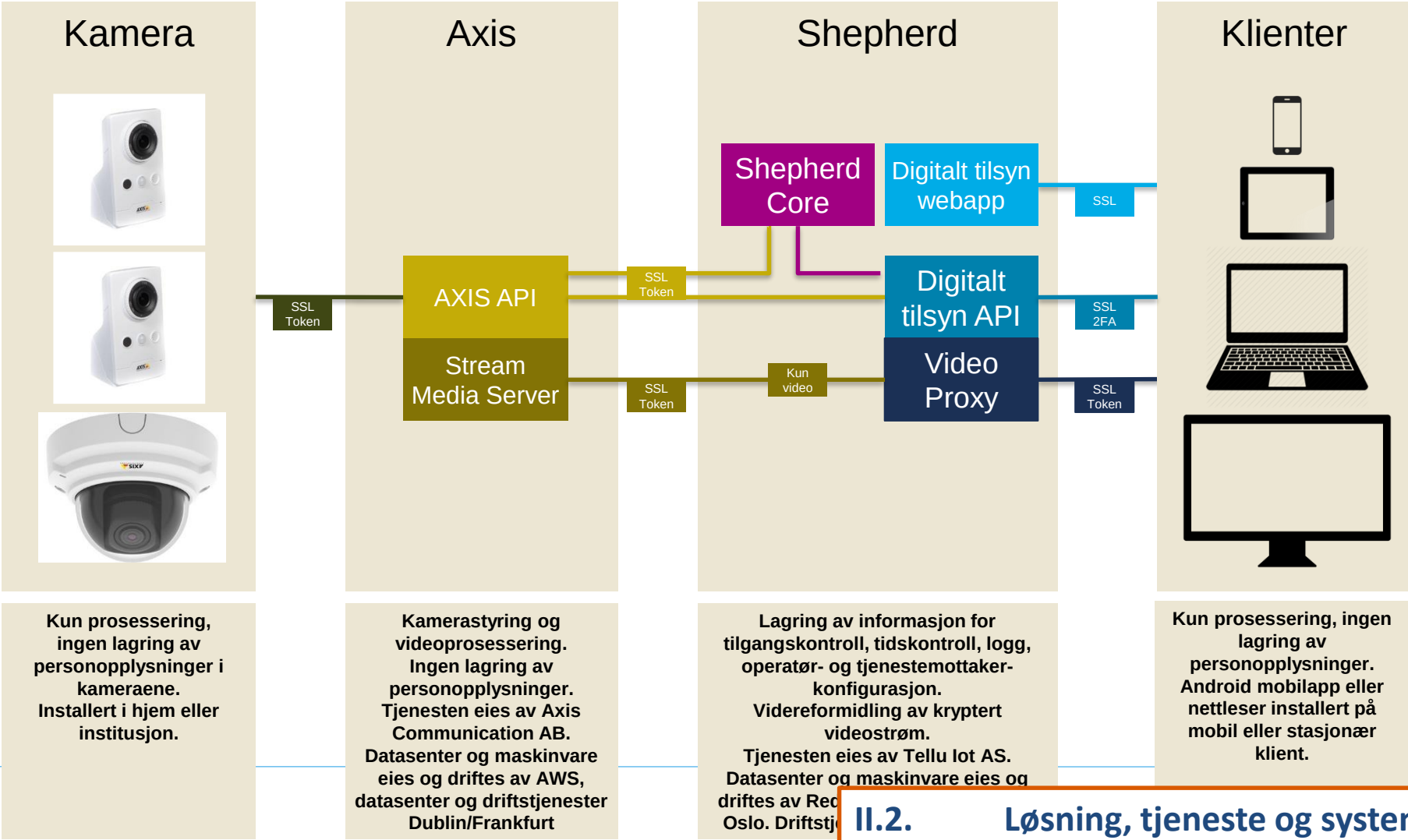
1. Vurdere å videreføre eller avslutte tjenesten selv om bruker havner på korttidsopphold eller sykehjem.
2. Hjemmetjenesten avslutter tjenesten og tiltak i profil.
3. Mail med avslutning skjema sendes til lin.hjelp.profil@lindesnes.kommune.no for å avslutte tilgangsstyring i web systemet
4. Hjelpemiddelkoordinator: Nullstiller og klargjøre kamerat til ny bruker. Avsluttes i web plattformen
5. Teknologien vaskes med overflatesprit og plasseres i lokalt lager.

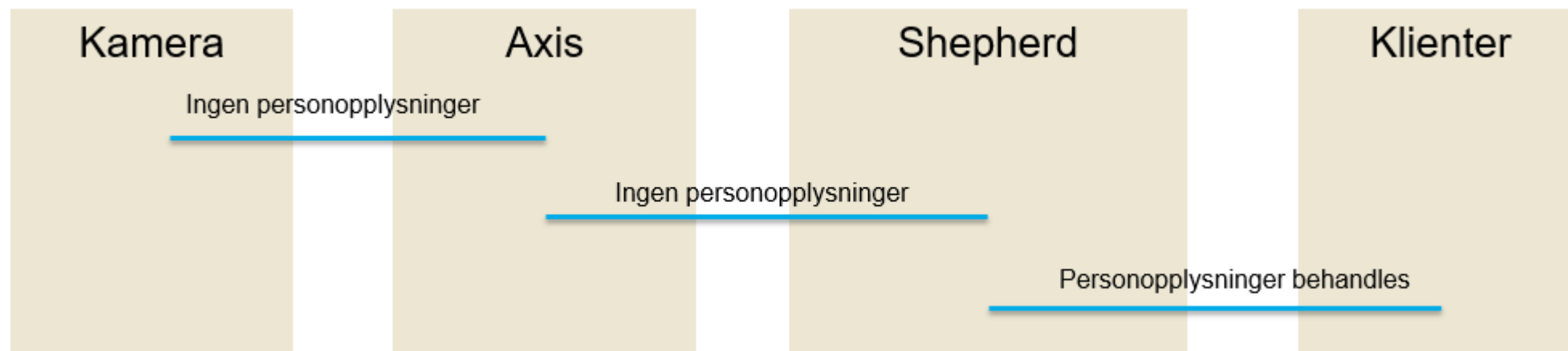


Teknisk skisse av digitalt tilsyn med Axis og Shepherd



Behandling av personopplysninger i Digitalt tilsyn





Behandlingens omfang



- **Følgende faktorer bør vektlegges:**
 - Antall registrerte involvert (i tall eller prosentandel av utvalget)
 - Volumet av data (antall variabler, detaljeringsgrad)
 - Lagringstid (kort, tidsavgrenset, permanent)
 - Geografisk omfang (lokalt, regionalt, nasjonalt, internasjonalt, globalt)



II.3. Behandlingens omfang



- **Beskrivelse av alle opplysninger som behandles**
 - Det innhentes personopplysninger ved søknad som blir registrert i EPJ. ([Søkandsskjema Helse- og omsorgstjenester Lindesnes](#))
 - I Axis systemet registreres løpenummer/navn på bruker.
 - Digitalt tilsyn blir ikke lagret, er øyeblikksbilde/video som utføres av ansatte i helse- og omsorgstjenesten som er gitt tilgang av avdelings leder.
- **Kategorier av de registrerte**
 - Tjenestemottaker/pasienter som mottar helse- og omsorgstjenester fra kommunen.
- **Volumet av data (antall variabler, detaljeringsgrad).**
 - Antall registrerte:
 - Lindesnes 4 stk pr august 2019.
- **Frekvensen av behandlingen**
 - Innhentes ved søknad og kartlegging/vurdering om tjeneste, og tjenesten utføres etter avtale med tjenestemottaker/pasient.
- **Det geografiske omfanget**
 - Lokalt – i kommunen



Behandlingsprotokoll



Velferdstekn - Digitalt tilsyn

Tittel *

Velferdstekn - Digitalt tilsyn

Kommune (Behandlingsansvarlig)

Mandal

System

Velg et alternativ

Systemeier

Enhetsleder

Systemleverandør (Databehandler)

Velg et alternativ

Databehandleravtale

Ja (lenke til databehandleravtale vedlagt)

Tjenesteområde

Helse og omsorg

Kommunal tjeneste

Velg et alternativ

Formål

For å kunne gi en faglig forsvarlig tjeneste til bruker uten å være fysisk tilstede

Behandlingsgrunnlag

Samtykke (skal være aktivt, frivillig og informert - legg ved samtykkeskjema)

Lovhjemmel

Helsepersonelloven kap. 8, §39-40

Helse- og omsorgstjenesteloven §3-2, pkt. 6a



Behandlingsprotokoll



Type registrerte

Pasienter

Antall registrerte

0-10

Personopplysninger

Navn, Bilde

Sensitive personopplysninger

Ja- opplysninger om helseforhold, Ja - Opplysninger som etter sin mengde eller art er følsomme

Hvor innhentes personopplysningene fra?

Fagsystem

Hvem har tilgang til opplysningene?

Brukere med spesiell tilgang

Hvor lagres personopplysningene?

I fagsystemet

Lagring

Etter arkivloven, Så lenge de registrerte benytter seg av tjenesten

Sletting

Opplysningene slettes ikke

Utlevering til tredjepart

Ingen utlevering til tredjepart



Behandlingsprotokoll



Sikkerhetstiltak - tekniske

kryptering, tilgangsstyring, totrinns pålogging, passord, sporing av endringer

Sikkerhetstiltak - organisatoriske

Meldesystem for avvik, Opplæring av ansatte, Tilgangsstyring, Involvering av personvernombud

Personvernkonsekvensutredning (DPIA)

DPIA er ikke gjennomført

ROS-analyse

ROS-analyse er gjennomført - DPIA må gjennomføres

Dokumenter

Databehandleravtale, ROS-analyse, Samtykkeskjema

Vedlegg

Legg til eller fjern vedlegg



Behandlingens formål



- Forsikre deg om at alle formål er beskrevet, det vil si at det er tydelig hva personopplysningene er planlagt å brukes til.
- Dersom formålet med bruken er av en slik art at det kan resultere i en inngripen i den private sfære, kan det være moment som taler for at risikoen er høy
- Dette omfatter for eksempel:
 - Vil det være kontrollformål (for eksempel skatt, NAV, toll, politi, forsikring)?
 - Vil formålet være å treffe avgjørelser om enkeltpersoner basert på systematisk og omfattende analyse av personlige aspekter?
 - Vil behandlingen av personopplysninger ha som mål å ta beslutninger som får betydning for den registrerte?



II.4. Formålsbeskrivelser



- Behandlingsprotokoll:

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Hva er formålet med behandlingen?	Formålet med digitalt tilsyn (kamera) er å kunne erstatte fysiske tilsyn. Det gir kvalitetsgevinst for tjenestemottaker, pårørende og kommunen; ingen lyder eller bevegelser som forstyrrer nattesøvn samt raskere respons ved plutselige behov. Digitalt tilsyn gir trygghet for bruker og pårørende.
2.	Vil formålet være å treffe avgjørelser om enkeltpersoner basert på systematisk og omfattende analyse av personlige aspekter?	Nei
3.	Vil behandlingen av personopplysninger ha som mål å ta beslutninger som får betydning for den registrerte?	Ja – ved endring i behov kan det medføre ett endret tjenestetilbud fra kommunen.
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?	Nei



Sammenheng behandlingen utføres i (kontekst)



- I noen sammenhenger behandles det kun trivielle personopplysninger og det er i hovedsak den registrerte som har kontroll over opplysningene.
- I andre sammenhenger behandles det sensitive personopplysninger og den registrerte har ingen medbestemmelse i hvilke opplysninger som registreres.
- Sammenhenger som tilsier at risikoen kan være høy, er sammenhenger hvor den registrerte har en klar forventning om personvern knyttet til behandlingen av personopplysninger.
- **Eksempler på slike sammenhenger er:**
 - forventning om konfidensialitet (for eksempel helse, velferd og arbeidsforhold)
 - forventning om privatliv (for eksempel i hjemmet og på rekreasjon)
 - behandling av personopplysninger fra ulike datasett og som er innsamlet for ulike formål, for ulike behandlingsansvarlige. Dette kan være uoversiktlig og uforutsigbart for den registrerte.



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



Nr.	Vurderingsspørsmål		Svar (forklar svar)
1.	Vil det behandles personopplysninger fra ulike datasett, som er innsamlet for ulike formål og fra ulike behandlingsansvarlige?		Nei
2.	Hvilke kilder brukes for innhenting av personopplysninger?		Tjenestemottaker, pårørende, søknad, folkeregisteret, EPJ
3.	a.	Kobles systemene der opplysninger behandles opp mot andre informasjonssystemer?	Nei
	b.	Finnes det tidligere erfaring med tilsvarende type behandling?	Ja, har hatt Digitalt tilsyn tjeneste siden januar 2017, fra Norsk Telemedisin.
4.	Finnes det noen nåværende tilfeller av allmenn bekymring for den beskrevne måten å behandle personopplysninger på?		Nei



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



5.	Hvilken relasjon har den behandlingsansvarlige med de registrerte? Beskriv maktforholdet mellom dem.	Ansvar for helse- og omsorgstjenestene i kommunen, mens tjenestemottaker er mottaker av tjenester. Offentlig instans mot privatperson.
6.	Med tanke på at kompleksitet i den sammenheng behandlingen utføres i (kontekst), i hvilken grad har de registrerte kontroll over sine opplysninger?	Den registrerte får vedtak, kopi av avtale og kan be om innsyn i journal.
7.	Beskriv hvordan behandlingen vil oppfattes fra den registrertes synsvinkel. Kan for eksempel de registrerte oppfatte behandlingen som lite forutsigbar?	Behandling utfra avtale om når og hvor ofte, som finnes på intranett i kommunen.
8.	Vil den registrerte ha en særskilt forventning om konfidensialitet (for eksempel dersom det omhandler helse, velferd, arbeidsforhold, kommunikasjon, lokasjon)?	Ja. Ansatte har taushetsplikt og underskrevet avtale om det.



Databehandleravtalen



- I Innføring velferdsteknologi Agder har kommunene i dag 2 databehandleravtaler:
 1. Databehandleravtalen med Telenor (ble signert som en del av kontrakten)
 1. Vedlegg med underleverandør
 2. Databehandleravtalen med responscenteret (vedlegg til samarbeidsavtalen)

IV.5. Ansvarsforhold

IV.4. Innebygd personvern



Behandling av personopplysninger er overordnet beskrevet i Tjenestespesifikke databehandlervilkår

01.07.2018



Tjenestespesifikke databehandlervilkår for behandling av personopplysninger

Axis Digitalt tilsyn

Telenors leveranse av 'Axis Digitalt tilsyn' («Tjenesten») kan innebære behandling av personopplysninger på vegne av kunden. For denne Tjenesten er Telenor da databehandler, og kunden er behandlingsansvarlig under personopplysningsloven.

Når Telenor er databehandler på vegne av kunden er behandlingen av personopplysninger regulert av særskilte databehandlervilkår. Databehandlervilkårene er angitt i Databehandlervilkårene mellom kunden og Telenor Norge AS («Databehandlervilkårene»).

For tjenester hvor Kunden delvis eller i sin helhet er behandlingsansvarlig er det Kundens ansvar å sikre lovlig formål og rettslig grunnlag (hjemmel) for behandlingen av personopplysninger. Kunden skal også sikre at egne brukere av Tjenesten er informert om Tjenesten og hvordan denne fungerer.

Oversikten under inneholder opplysninger som er av relevans for Partenes oppfølging av databehandlervilkårene.

Navn på tjeneste/prosess regulert av Databehandlervilkårene	Axis Digitalt tilsyn
Hva er formålet med databehandlers behandling av personopplysninger på vegne av behandlingsansvarlig?	Yte helse- og/eller omsorgstjenester vha velferdsteknologi på vegne av en kommune eller annen aktør med ansvar for å yte helse- og/eller omsorgstjenester. Mer spesifikt å yte administrasjon, drift og vedlikehold av digitale kamera og tilhørende kommunikasjonsenheter, samt datagrunnlag for kvalitetssikring og -forbedring av tjenesten.
Hvilke typer av helse- og personopplysninger behandles?	Personalia om tjenestemottaker: Kommunen kan registrere fullt navn eller fødselsnummer, men kan også anvende pseudonym for identifisering av tjenestemottaker. Tilsynshendelser og -historikk: tidspunkt, operatør, videostrøm, stillbilder. Enhetsinformasjon: serienummer, plassering Personalia om kundens administratører og helsearbeidere: fullt navn, virksomhet, rolle, fødselsnummer (for autentisering).
Hvordan behandler Databehandler personopplysningene?	Personopplysninger behandles kun digitalt. Tilsyn gjennomføres fra webapplikasjon i nettleser. Ingen personopplysninger lagres på pc/nettbrett/mobil. Tilgangskontroll, tidskontroll, logg, operatør- og tjenestemottakerkonfigurasjon lagres i Telenors integrasjonstjeneste Shepherd.

Telenor Norge AS

Side 1 av 3

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?	Henviser til databehandleravtalen
b.	sikker koding?	
c.	testing og godkjenning før produksjonssetting?	
d.	kontinuitets- og beredskapsplaner?	
e.	jevnlig revisjoner?	
f.	opplæring?	Opplæring med leverandør og internopplæring.
2.	Er alle prinsippene for behandling av personopplysninger ivaretatt i løsningen? – Se DEL V.1	Ja, se DEL V.1
3.	Hvordan er den registrertes rettigheter ivaretatt i løsningen? – Se DEL V.2 for hvilke rettigheter er det snakk om.	Er ivaretatt se DEL V.2
4.	Tas ny teknologi i bruk?	JA Se DEL VI.1.1. og VI.1.2.
5.	Brukes eksisterende teknologi på en ny måte?	Ja – Se DEL VI.1.1. og VI.1.2.



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?	Databehandleravtalen med Telenor, og med underleverandør <u>Tellu</u>
	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
3.	Om databehandleravtalen:		
	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



Skal det merkes at det er kamera?



- Skal det merkes med kameraovervåking når det utføres digitale tilsyn i private boliger? Evt. skal det merkes på utsiden? På rommet hvor kameraet er?
- Innspill fra brukerrepresentant er at det ikke er ønskelig med merking som er synlig pga at det oppleves som stigmatiserende.



[Veileder fra Datatilsynet-
kameraovervåking](#)



Arbeidsoppgave fase 1



1. Vurdering av personvernkonsekvens utfra tabell på s 8

- Stikkord:
 - Ros analyse - Behandlingsprotokoll – Tjenesteforløpet – Prosedyrer - databehandleravtaler



DEL I. Vurdering av behov for DPIA



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

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

Forsett videre



Arbeidsoppgave fase 1



1. Vurdering av personvernkonsekvens utfra tabell på s 8
 2. Gjøre en systematisk beskrivelse av behandlingen
 1. Hva har vi...
 2. Hva mangler vi...
 - Art, omfang, formål, sammenheng
 - Kilder og mottagere
 - Informasjonssikkerhet
 - Ansvarsforhold
- Stikkord:
 - Ros analyse - Behandlingsprotokoll – Tjenesteforløpet – Prosedyrer - databehandleravtaler



Forløp/prosess



Veileder fra
Datatilsynet

Sjekkliste fra
Datatilsynet

Rettslig
grunnlag

Behandlings
protokoll

Personvern
prinsipper

Mal for DPIA

Den
registrertes
rettigheter
og friheter

Mal for
Ros analyse



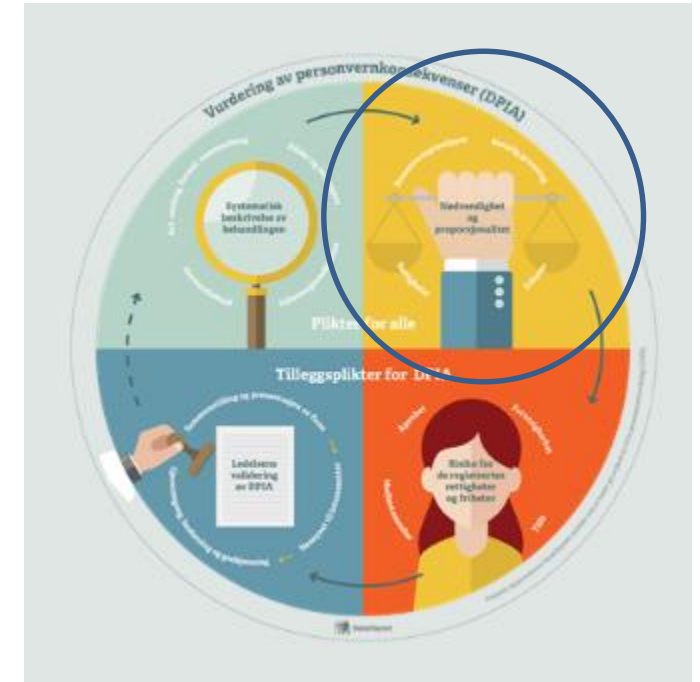
Fase 2



Ny gjennomgang av valgene for å se til at de bidrar til at behandlingen er nødvendig og står i et rimelig forhold til formålene, for å etterleve lovkravene.

Nødvendighet og proporsjonalitet

- Personvernprinsipper
- Rettslig grunnlag
- Friheter
- rettigheter



Personvernprinsipper



- **Formålsbegrensning:**

- Formål(ene) skal være spesifikt, uttrykkelig angitt og berettiget (artikkel 5.1 bokstav b).

- **Sjekk følgende:**

- Er formålet klart definert? Er formålet definert slik at det samsvarer med forventningene til de registrerte?
 - Vurder om formålet kan oppnås med en mindre inngripende behandling.
 - Vurder hvorvidt formålet kan oppnås med anonyme eller pseudonyme alternativer.



Del V. Nødvendighet og forholdsmessighet av behandlingen



V.1. Personvernprinsippene – punkt 2

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
c.	Finnes det mindre personverninnngripende alternativer for å oppnå det samme formålet?	Nei Tjeneste vurderes utfra tjenestemottakers behov og ønsker, og minst innngripende tiltak.
D	Vurder hvorvidt formålet kan oppnås med anonyme eller pseudonyme alternativer.	Ikke aktuelt



Personvernprinsipper



Lagringsbegrensning:

- Personopplysninger skal slettes eller anonymiseres når formålet er oppnådd (artikkel 5.1 bokstav e).
 - **Vurder** om personopplysninger lagres etter at formålet er oppnådd.
 - Vurder hver enkelt kategori av personopplysninger.
 - Vurder når sletting inntreffer.
 - Vurder eventuelt når personopplysninger anonymiseres eller pseudonymiseres.
 - **Vurder** hvilke garantier som må være plass dersom personopplysninger skal lagres i lenger perioder grunnet arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål (artikkel 89 nr. 1).



IV.1. Oversikt over behandling og behandlingsaktiviteter



Punkt 2: Lagring:

2.	Lagring	Ikke lagring på kamera Noen personopplysninger i systemet. (Henviser til Behandlingsprotokoll tjenesteforløpet, og søknad om helse- og omsorgstjenester.)
----	---------	--



IV.2.2. Lagring



Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Hvordan skal opplysningene lagres?	Digitalt tilsyn (bilde, lyd) lagres ikke. Navn/løpenummer i EPJ, og loggføring lagres i henhold til gjeldende lovverk. (Arkivloven § 1)

2.	Hvor og hvor lenge lagres personopplysningene?	Personopplysninger lagres i EPJ, <u>ProAlert</u>, <u>Shepard</u>. Opplysninger lagres etter gjeldende lovverk. (Arkivloven § 1)
3.	Hvilke kriterier brukes for å bestemme lagringstid?	Henviser til gjeldende lovverk/prosedyre for lagring (Arkivloven § 1)
4.	Når skal personopplysningene slettes?	Henviser til gjeldende lovverk/prosedyre for sletting
5.	Etter at formålet ved behandlingen er oppnådd, hvor lenge lagres personopplysningene før de slettes?	Henviser til gjeldende lovverk/prosedyre for sletting
6.	Er det utarbeidet rutiner for sletting?	Henviser til prosedyre for sletting som finnes på intranett i kommunen
7.	Gis det informasjon til den registrerte om muligheten til å slette opplysninger og hvordan sletting kan gjøres?	Ja. Informasjon gis via vedtak om helse- og omsorgstjeneste

Personvernprinsipper





V.1. Personvernprinsippene

Punkt 5: Lagringsbegrensning:

5	Lagringsbegrensning		
	a.	Vurder om personopplysninger lagres etter at formålet er oppnådd og når opplysningene slettes.	Gjeldende lovverk, tidligere beskrevet
	b.	Vurder når personopplysninger anonymiseres eller pseudonymiseres som muliggjør videre lagring.	Ikke aktuelt
	c.	Vurder hvilke garantier som må være plass dersom personopplysninger skal lagres i lenger perioder grunnet arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål (GDPR art.89 nr.1).	Ikke aktuelt



Prosedyrer



- ***Tilgang til ansatt i system***
- ***Oppstart ny tjenestemottaker, og avslutning av tjenestemottaker.***
- ***Oppfølging logg – internkontroll***
 - *Følgende skal tas vare på til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem:*
 - *Logger med sikkerhetsmessig betydning, herunder registrering av autorisert bruk og forsøk på uautorisert bruk av informasjonssystemene. (Normen 5.3 s 15)*





- **Spørsmål:**
 - *Er logg over alle hendelser fra f.eks. kamera journalpliktig i EPJ?*
 - *Tilsynene blir dokumentert i EPJ. Må også logg arkiveres i EPJ?*
- Tilgangslogg – internkontroll prosedyre
- Teknisk logg – nei
- Tilsynslogg – I EPJ (alle tilsyn blir logget)
 - Hvor ofte logg gjennomgang? (bør inkluderes i andre revisjoner/gjennomganger som gjøres i kommunen)

Personvernprinsipper



- **Dataminimering:**

- Personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålene (artikkel 5.1 bokstav c)
- Vurder personopplysningene som skal behandles. Kan formålet oppnås ved for eksempel:
 - å begrense innsamling av personopplysninger?
 - med mindre detaljerte personopplysninger?
 - uten fortrolige eller sensitive personopplysninger?
- Begrunn nødvendighet og relevans relatert til formål for hver enkelt variabel i et datasett.



V.1. Personvernprinsippene



- **Punkt 3: Dataminimering:**

3	Dataminimering.	
	Kan formålet oppnås ved for eksempel:	
	a.	å begrense innsamling av personopplysninger?
	b.	med mindre detaljerte personopplysninger?
	c.	uten fortrolige eller sensitive personopplysninger?
	Begrunn nødvendighet og relevans relatert til formål for alle opplysninger som behandles.	
	Alle personopplysninger er relevante for formålet	



Personvernprinsipper



Riktighet:

- Personopplysninger skal være korrekte og oppdaterte (artikkel 5.1 bokstav d)
 - **Vurder** hvordan personopplysninger holdes korrekte og oppdaterte, med og uten den registrertes involvering.
 - **Vurder** om dere har nødvendig funksjonalitet for å rette og slette uriktige personopplysninger.
 - Ut i fra den registrertes perspektiv, er det behov for kontradiksjon?
 - Det vil si den registrertes anledning til å imøtegå det den behandlingsansvarlige har registrert.
 - Et eksempel er en saksbehandlers beskrivelse av en samtale eller et møte som kan ha elementer av subjektiv oppfattelse av uttalelser, meninger, stemning eller observasjon.
 - Har dere rutiner for hvordan ansatte fører journaler, notater, møtereferat og så videre?



V.1. Personvernprinsippene



Punkt 4: Riktighet

4	Riktighet	
a.	Vurder hvordan personopplysninger holdes korrekte og oppdaterte, med og uten den registrertes involvering.	Jevnlig oppdatering av brukerkort og tiltaksplan i system. Primærkontakt ansvarlig.
b)	Vurder om det finnes nødvendig funksjonalitet for å rette og slette uriktige personopplysninger, ref. punkt IV.2.5 og IV.2.6.	Ja, leverandør kan rette/slette
c.	Har dere rutiner som ivaretar kravet til korrekte og oppdaterte personopplysninger?	Ja, automatisk oppkobling mot folkeregisteret. Jevnlig oppdatering av brukerkort og tiltaksplan i system. Primærkontakt ansvarlig.



De registrertes rettigheter



Vurder hvordan de registrertes rettigheter ivaretas:

- **Vurder** hvordan informasjon til de registrerte gis (rettferdig og gjennomiktig behandling, artikkel 12, 13 og 14).
- **Vurder** innhenting av samtykke (artikkel 7 og 8).
 - Er det frivillig, uttrykkelig, spesifikt?
 - Dokumenteres samtykke?
 - Kan samtykke trekkes tilbake like enkelt som det gis?
 - Kontroller at samtykke ikke sammenblandes med kontrakt eller personvernerklæring.
- **Vurder** hvordan den registrertes rett til innsyn og til dataportabilitet ivaretas (artikkel 15 og 20).
- **Vurder** hvordan den registrertes rett til korrigering og sletting ivaretas (artikkel 16 og 17).
- **Vurder** hvordan den registrertes rett til innsigelser og begrensning av behandling ivaretas (artikkel 18, 19 og 21).
- **Vurder** hvordan forbud mot automatiserte individuelle avgjørelser, herunder profilering håndheves (artikkel 22).

Kontroller om det er nødvendig eller mulig å forbedre måten de registrertes rettigheter ivaretas. Der det er mulig, gjennomgå beskrivelsen på nytt eller foreslå ytterligere tiltak.



V.2. Ivaretagelse av de registrertes rettigheter



Vurder hvordan de registrertes rettigheter ivaretas:

Nr.	Vurderingstemaer	Vurdering
1.	Vurder hvordan informasjon til de registrerte gis (prinsippet om rettferdighet og åpenhet i behandlingen) (GDPR art.12, 13 og 14).	Godt ivaretatt. Informasjon gis skriftlig og muntlig
2.	Vurder hvordan den registrertes rett til innsyn ivaretas (GDPR art.15).	Godt ivaretatt. Skriftlig og muntlig informasjon
3.	Vurder hvordan den registrertes rett til retting og sletting ivaretas (GDPR art.16 og 17).	Godt ivaretatt.
4.	Vurder hvordan den registrertes rett til innsigelser og begrensning av behandling ivaretas (GDPR art.18, 19 og 21).	Ikke aktuelt
5.	Vurder hvordan den registrertes rett til dataportabilitet ivaretas (GDPR art.20).	Ikke aktuelt
6.	Vurder hvordan forbud mot automatiserte individuelle avgjørelser, herunder profilering håndheves (GDPR art.22).	Ikke aktuelt



De registrertes 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

Kontroller om det er nødvendig eller mulig å forbedre måten de registrertes friheter tas hensyn til.

Der det er mulig, gjennomgå beskrivelsen på nytt eller foreslå ytterligere tiltak.



V.3. Ivaretagelse 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	Godt ivaretatt. Henvis til taushetsplikt, avtale, etc. Digitalt tilsyn vurderes som mindre inngripende i privatlivet enn fysisk tilsyn.
	Retten til ikke å bli diskriminert	Ikke relevant
	Tanke-, tros- og religionsfrihet	Ikke relevant
	Ytrings-, og informasjonsfrihet	Ikke relevant



Rettigheter



Rettslig grunnlag

- Er behandlingen basert på lovlighet, rettferdighet og åpenhet (artikkel 5.1 bokstav a og artikkel 6 og 9)?
 - Kommer det rettslige grunnlaget/behandlingsgrunnlaget tydelig frem? For eksempel samtykke, nødvendig for avtale/kontrakt, rettslig forpliktelse, vitale interesser, utøvelse av offentlig myndighet, berettiget interesse.
 - Omfatter rettslig grunnlag både egne formål og utlevering?
 - Har dere vurdert og kontrollert behandlingsgrunnlagets gyldighet og rimelighet?
 - Hva er forventede fordeler ved behandlingen? For virksomheten, den registrerte, samfunnet for øvrig og så videre.
 - Skiller dere tydelig mellom hvilke personopplysninger som er om er nødvendig for avtale og hva som skal baseres på samtykke?
 - **Vurder** hvordan åpenhet ivaretas i behandlingen.





DEL III. Behandlingens lovlighet

Behandlingens lovlighet er beskrevet i behandlingsprotokollen

• III.1. Hjemmelsgrunnlag

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Finnes det hjemmelsgrunnlag i forskrift eller lov for behandlingen av personopplysninger?	Ja Helsepersonell loven <u>kap 8 § 39-40</u> Helse- og omsorgstjenesteloven § 3-2 pkt. 6a
2.	Finnes det annet rettsgrunnlag for behandlingen (for eksempel samtykke, avtale, verne vitale interesser, utførelse av myndighetsoppgave, oppfylle rettslig forpliktelse, jf. GDPR art.6)?	Nei
3.	Finnes det konsesjon eller forhåndsgodkjenning fra REK (Regional etisk <u>komitè</u>) eller Datatilsynet, eller dispensasjon fra taushetsplikten?	Nei



DEL III. Behandlingens lovlighet



• III.2. Samtykke

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Forutsettes det samtykke for behandlingen?	Nei, tjenestemottaker søker om helse og omsorgstjeneste.
2.	Hvordan vil samtykke bli innhentet?	
3.	Er alle kravene til samtykke oppfylt? Samtykke fra den registrerte må være frivillig, spesifikk, informert og utvetydig (GDPR art.4).	
4.	Dokumenteres samtykke?	
5.	Kan samtykke trekkes tilbake like enkelt som det gis?	
6.	Foreligger det informasjon til den registrerte om muligheten til å trekke tilbake samtykke?	
7.	Omfatter samtykket alle behandlinger og behandlingsformål som nevnt i DEL IV?	

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



DEL III. Behandlingens lovlighet



• III.3. Viderebehandling

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Behandles opplysninger videre til andre formål enn opprinnelig formål (for eksempel forskning)?	Hvis ja, beskriv viderebehandlingene og hvilke opplysninger som videre behandles.
2.	Dersom rettsgrunnlag for opprinnelig behandling av personopplysninger er lov eller forskrift, åpner lov eller forskrift for viderebehandling av personopplysninger?	
3.	Dersom opprinnelig behandling er basert på samtykke, dekker samtykket viderebehandlingen av de samme personopplysningene?	Hvis svaret er nei, vil det innhentes nytt samtykke?
4.	Videre behandles personopplysninger for statistiske formål?	Hvis ja, finnes det nødvendige garantier for å ivareta personvernet? Nevn garantier.

NB: Undersøk lovverk iht uthenting statistikk



DEL III. Behandlingens lovlighet



• III.4. Vurdering av formålet sett opp mot rettsgrunnlag

Nr.	Vurderingsspørsmål	Svar (forklar svar)
1.	Er formålet eller formålene klart definert?	Ja
2.	Er formålet nedfelt i forskrift eller lov?	Ja
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
5.	Er formålet beskrevet i løsning, tjeneste eller system utfordrende sett opp mot rettsgrunnlaget?	Nei
6.	Omfatter rettslig grunnlag både egne formål og utlevering?	Nei
7.	Er formålet definert slik at det samsvarer med forventningene de registrerte kan ha ut fra egen forskrift, lov eller samtykkevilkår?	Ja



Informasjonsbrev og avtale skjema



Lindesnes kommune



Informasjonsbrev til brukere med digitalt tilsyn (kamera)

Lindesnes kommune vil de kommende årene jobbe målrettet mot økt bruk av velferdsteknologi. Vi kan derfor gi deg som bruker av tjenesten mulighet å få tilsyn med hjelp av kamera, som et trygt og diskret alternativ til fysisk tilsyn i hjemmet.

Tilsyn ved hjelp av kamera medfører flere fordeler:

- Flere og oftere tilsyn i løpet av døgnet
- Raskere respons ved plutselige behov
- Ingen hyder eller bevegelser som forstyrrer nattesøvnen
- Økt trygghet for bruker og pårørende

Digitalt tilsyn innebærer at ordinære tilsyn erstattes av et «besøk» gjennom kamera, som gjennomføres ved bestemte tider av ett kommunalt responscenter i Agder. For deg betyr det at det er kvalifisert helsepersonell på responscenteret som utfører digitalt tilsyn på natten etter avtalte tidspunkt. Det vil allikevel bli som før, at hjemmesykepleien vil bli oppringt av responscenteret og kommer hjem til deg når det er behov for det. Kommunalt responscenteret er åpent hele døgnet og gjennom hele året.

Digitalt tilsyn via kamera krever tilgangskontroll og alle tilsyn blir loggført med tidspunkt og navn på den som utførte tilsynet. Ingen film lagres under tilsynet.

Vi håper at du vil bli fornøyd med den nye løsningen.

Dersom du har spørsmål kan du kontakte

Lindesnes kommune;
Daglig leder tlf. xxxx xxxx

Mvh (daglig leder navn)
Elektronisk sig.

Lindesnes kommune



Avtale skjema til brukere med tilsyn av nattkamera

Det avtales herved:

Lindesnes kommune og Responscenter Kristiansand skal føre tilsyn med hjelp av nattkamera til undertegnede bruker inntil videre.

Tilsyn skal foregå på følgende måte:

	Forklaring	Beslutning
Intervall	Hvilke dager og tidspunkt skal tilsynet skje	
Ved feil	Hvordan skal tilsyn utføres ved feil på nattkamera	

Både Lindesnes og undertegnede bruker kan når som helst avbryte nattkamera-tjenesten og gå tilbake til ordinære fysiske tilsyn.

~~For~~ behov for hjelp vil natt- tjenesten i Lindesnes rykke ut til deg.

Dato/sted:

Navn:

.....

.....



Arbeidsoppgave fase 2



Ny gjennomgang av valgene for å se til at de bidrar til at behandlingen er nødvendig og står i et rimelig forhold til formålene, for å etterleve lovkravene.

Gjør en vurdering av:

1. Personvernprinsipper
2. Rettslig grunnlag
3. Friheter og Rettigheter er ivaretatt

Stikkord:

Behandlingsprotokoll – prosedyrer – informasjonbrev



Forløp/prosess



Veileder fra
Datatilsynet

Sjekkliste fra
Datatilsynet

Rettslig
grunnlag

ROS- analyse
med
utgangspunkt i
den registrertes
rettigheter og
friheter

Behandlings
protokoll

Personvern
prinsipper

Mal for DPIA

Den
registrertes
rettigheter
og friheter

Mal for
Ros analyse



Fase 3



I denne fasen skal man gjennomføre en vurdering av personvernkonsekvenser for den registrertes rettigheter og friheter.

Vurdering av risiko for:

- De registrertes rettigheter og friheter
- Planlagte tiltak for å håndtere risikoene





1. Medbestemmelse

den registrerte har ikke et valg, får ikke informasjon, får ikke innsyn, og så videre.

2. Manglende reell åpenhet

virksomheten evner ikke å forklare komplekse behandlinger eller forventet resultat ved sammenstilling av personopplysninger med andre datasett og så videre.

3. Manglende forutsigbarhet ved behandlingen

behandlingen er utenfor det den registrerte vil forvente og så videre.





- **Rett til ivaretagelse av konfidensialitet** - den registrerte har rett til at personopplysningene kun er tilgjengelig for dem som har tjenstlig behov
- **Rett til medvirkning** - den registrerte har rett til å medvirke i hvordan informasjonen behandles, og til hva
- **Rett til åpenhet** - den registrerte har rett på åpenhet rundt hvordan personopplysningene behandles og til hva.
- **Rett til ivaretagelse av integritet** - den registrerte har rett til at personopplysningene er korrekte til enhver tid
- **Retten til ivaretagelse av tilgjengelighet** - den registrerte har rett til at personopplysningene skal være tilgjengelige slik at informasjonsbehandlingen ikke forsinkes



VI.1. Risiko, konsekvenser og sannsynlighet



- VI.1.1. Sikkerhet ved behandlingen
- VI.1.2 Personopplysningsvernet



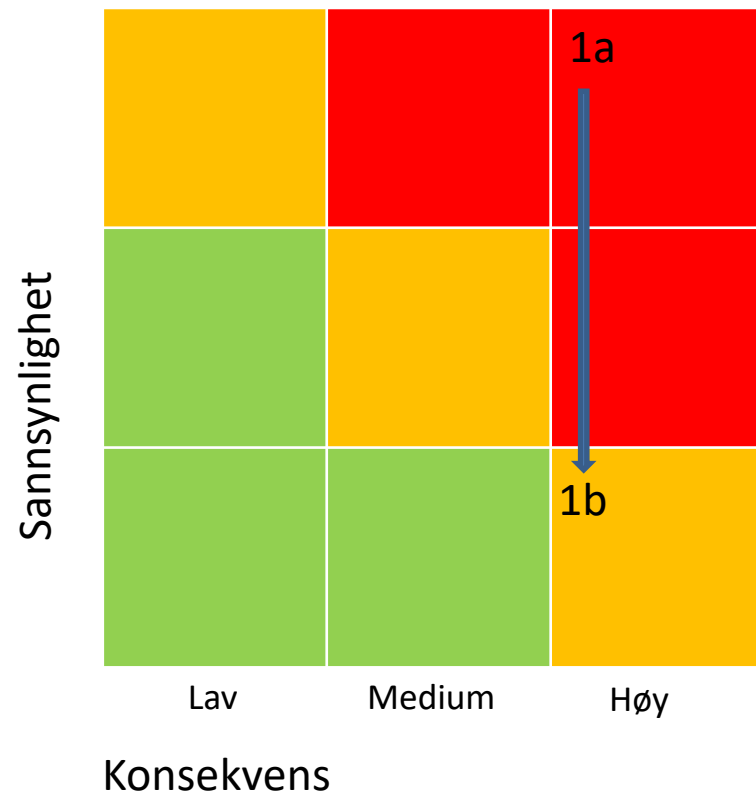


Rett til ivaretagelse av konfidensialitet

-den registrerte har rett til at personopplysningene kun er tilgjengelig for dem som har tjenstlig behov



Identifisert risikomoment	Sannsynlighet / Konsekvens (uten tiltak)	Risikoreducerende tiltak	Ny sannsynlighet / konsekvens (restrisiko etter tiltak)
Uvedkommende får tilgang til mine personopplysninger.	1 a: Høy sannsynlighet Høy konsekvens	• Overføringen av mine personopplysninger skjer kryptert innenfor et sikkert nett • Kommunen styrer hvem som har tilgang til mitt kamera, det føres logg over hvem som slår det på og hvor lenge det er slått på • De som har tilgang til mitt kamera må bruke 2-faktor pålogging • De som har tilgang til mitt kamera gjennomgår relevant opplæring • Mitt kamera er bare påslått i et begrenset tidsrom (som jeg har avtalt med kommunen) • Kommunen registrerer kun relevante og nødvendige personopplysninger om meg i sitt system • Kameratjenesten bruker ikke navnet mitt, kun ID-nummer • Både DDV og Telenor driver driftsovervåking av tjenesten • Det mitt kamera filmer blir ikke lagret, bare streamet	1 b: Lav sannsynlighet Høy konsekvens



Restrisiko:
1b lav/høy



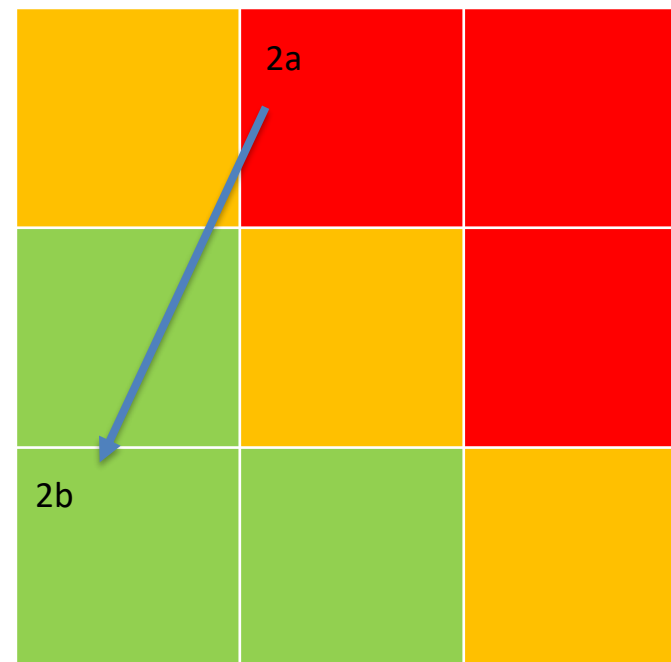


Rett til medvirkning

- den registrerte har rett til å medvirke i hvordan informasjonen behandles, og til hva

Identifisert risikomoment	Sannsynlighet / Konsekvens (uten tiltak)	Risikoreducerende tiltak	Ny sannsynlighet / konsekvens (restrisiko etter tiltak)
Jeg har ingen innflytelse på når eller hvordan mine personopplysninger behandles	2 a: Høy sannsynlighet Middels konsekvens	- Jeg har en skriftlig avtale med kommunen som regulerer i hvilke tidsintervaller kameraet mitt slås på og deltar i beslutninger rundt hva de skal gjøre dersom jeg for eksempel ikke er på rommet mitt i dette intervallet - Kameratjenesten kan avsluttes når jeg måtte ønske	2b: Lav sannsynlighet Lav konsekvens

Sannsynlighet



Lav Medium Høy

Konsekvens

Restrisiko: 2b
lav/lav

LINDESNES
KOMMUNE

- På lag med framtida



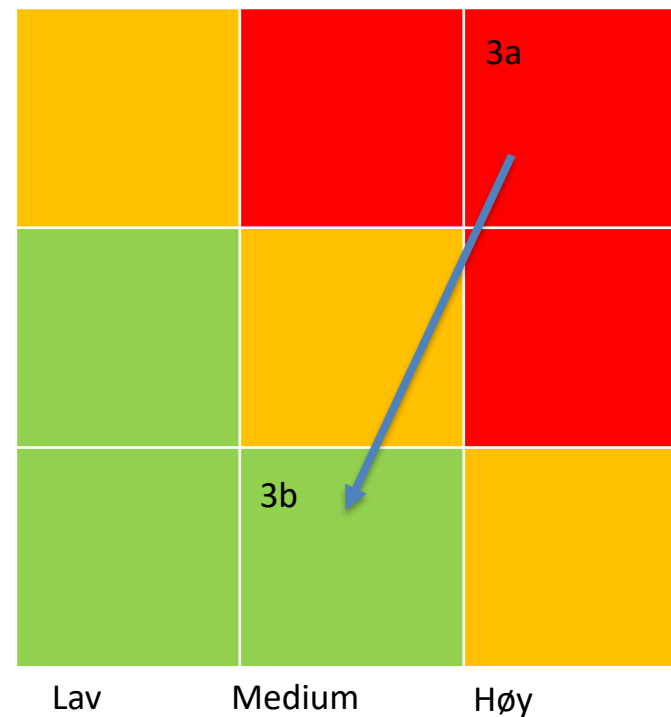
Rett til åpenhet

-den registrerte har rett på åpenhet rundt hvordan personopplysningene behandles og til hva.



Identifisert risikomoment	Sannsynlighet / Konsekvens (uten tiltak)	Risikoreduserende tiltak	Ny sannsynlighet / konsekvens (restrisiko etter tiltak)
Jeg vet ikke når eller hvorfor mine personopplysninger brukes	3 a: Høy sannsynlighet Høy konsekvens	- Jeg og mine pårørende får informasjonsskriv og opplæring før oppstart av kameratjenesten. <i>Kommunen har utarbeidet en personvernerklæring for kameratjenesten.</i> - Kommunen fører logg over bruk av mitt kamera som jeg har innsynsrett i (via min journal) - Kommunen har en oppdatert behandlingsprotokoll over behandling av personopplysninger som jeg har innsynsrett i.	3b: Lav sannsynlighet Middels konsekvens

Sannsynlighet



Konsekvens

Restrisiko: 3b
lav/medium

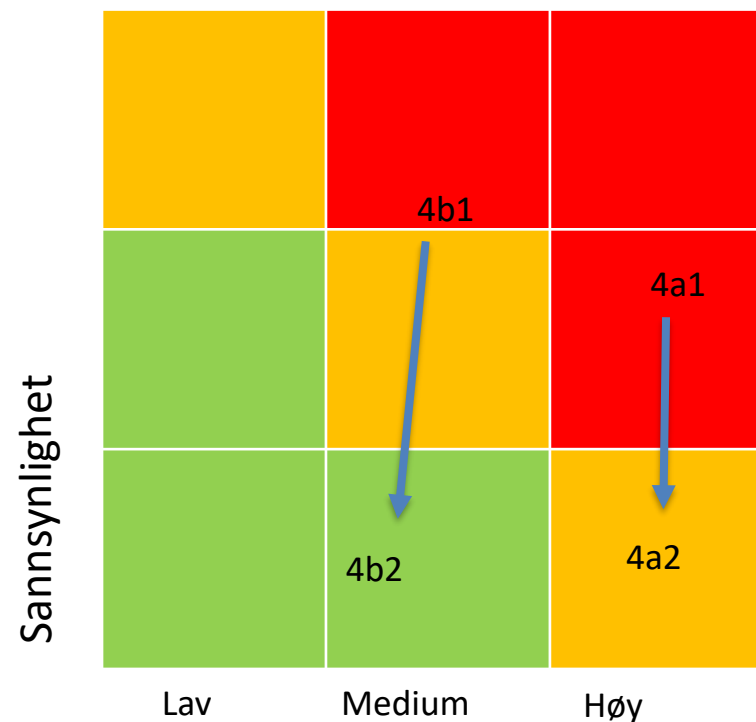


Rett til ivaretagelse av integritet

-den registrerte har rett til at personopplysningene er korrekte til enhver tid



Identifisert risikomoment	Sannsynlighet / Konsekvens (uten tiltak)	Risikoreduserende tiltak	Ny sannsynlighet / konsekvens (restrisiko etter tiltak)
1: Jeg får feil behandling fordi kommunen ikke har registrert korrekte opplysninger om meg	4a-1: Middels sannsynlighet Høy konsekvens	- Jeg får informasjon om hvilke opplysninger som registreres om meg når jeg inngår avtale med kommunen om digitalt tilsyn - Jeg og mine pårørende får informasjonsskriv og opplæring før oppstart av kameratjenesten.	4b-1: Lav sannsynlighet Høy konsekvens
2: Jeg mister tillit til kommunen	4a-2: Høy sannsynlighet Middels konsekvens	- Kommunen har egen prosedyre for oppdatering/retting/sletting av mine personopplysninger <i>Kommunen planlegger å innføre eSense som reduserer manuelle behandlinger av mine personopplysninger</i>	4b-2: Lav sannsynlighet Middels konsekvens



Restrisiko:
4 a 2 og 4 b 2

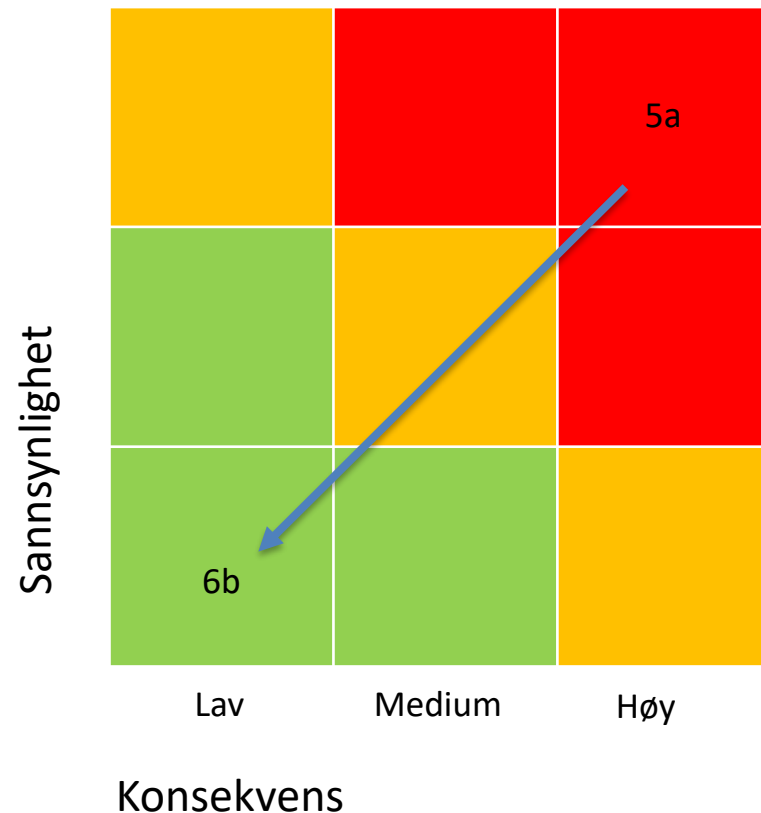


Retten til ivaretagelse av tilgjengelighet

-den registrerte har rett til at personopplysningene skal være tilgjengelige slik at informasjonsbehandlingen ikke forsinkes



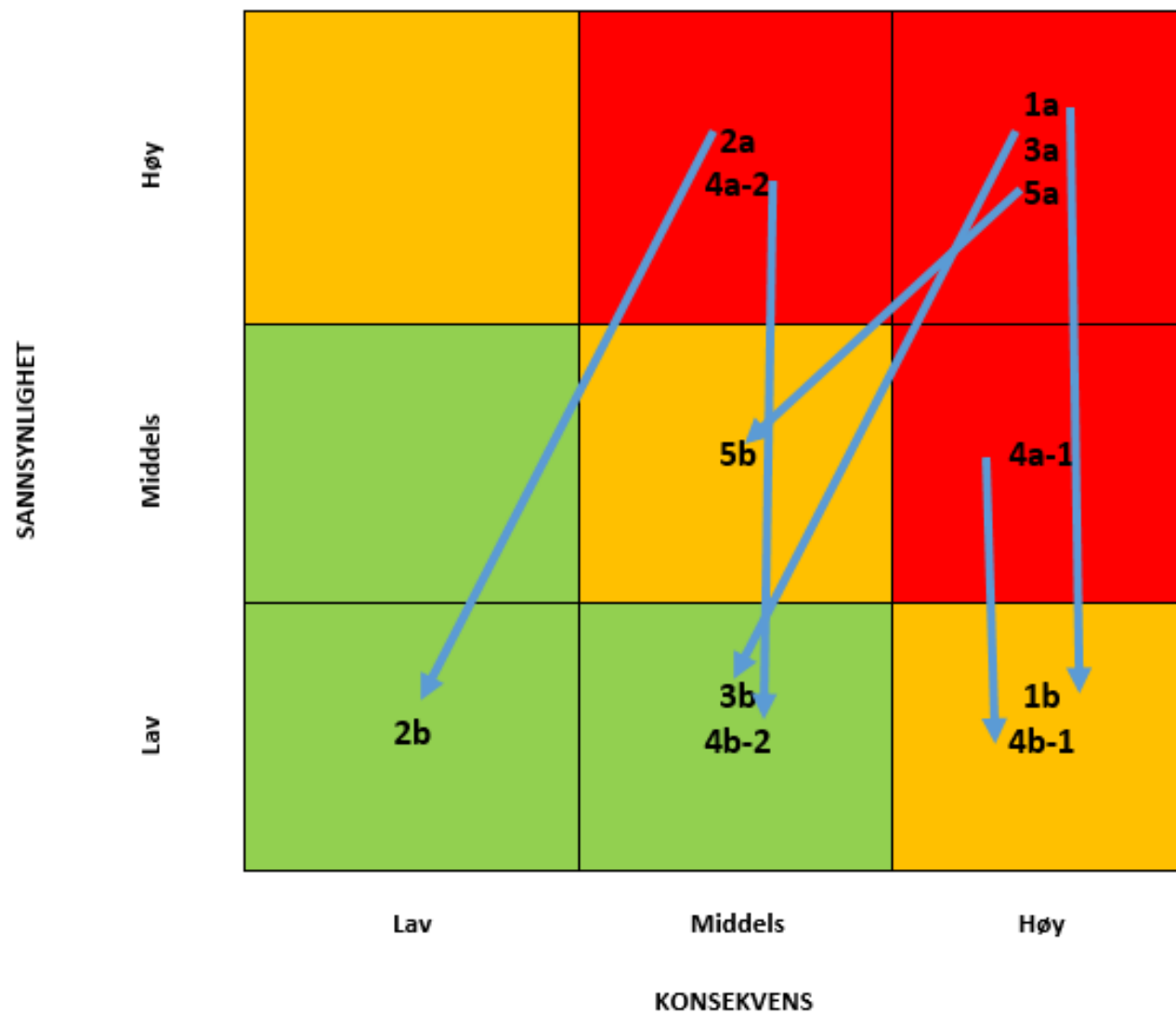
Identifisert risikomoment	Sannsynlighet / Konsekvens (uten tiltak)	Risikoreduserende tiltak	Ny sannsynlighet / konsekvens (restrisiko etter tiltak)
Kommunen får ikke utført det digitale tilsynet vi har avtalt fordi de ikke har tilgang til kameraet mitt. Dette kan bety at det tar lengre tid før jeg får den helsehjelpen jeg trenger dersom jeg for eksempel har falt ut av senga	5a: Høy sannsynlighet Høy konsekvens	- Jeg har en skriftlig avtale med kommunen om hvordan tilsyn skal utføres dersom det oppstår feil på kameraet mitt - Kommunen har prosedyrer for å gjennomføre manuelle tilsyn hos meg dersom digitalt tilsyn ikke er gjennomførbart. - Jeg og mine pårørende får informasjonsskriv og opplæring før oppstart av kameratjenesten. - Både DDV og Telenor driver driftsovervåking av kameratjenesten	5b: Middels sannsynlighet Middels konsekvens



Restrisiko: 6b
lav/medium



Oppsummering: a = opprinnelig risiko, b = restrisiko etter tiltak



Tiltak



- Velg tiltak for å håndtere risikoene for de registrertes og andre berørte personers rettigheter og berettigede interesser.
- Identifiser eller bestem hva slags tiltak (garantier, sikkerhetstiltak og mekanismer) som kan håndtere risikoene.



Slike tiltak kan typisk være:



Spesifikke garantier for å **minimere inngripen**.

- For eksempel:
 - **innhenting av registrertes/representanters syn på behandlingen**
 - **forsterket informasjonsplikt** (løpende informasjon, informasjon i flere kanaler, spesifikk informasjon om kobling mellom datasett og resultat av kobling og så videre).
 - **særskilte dataminimeringstiltak** (monitorering bare i bestemte tidsrom eller spesifikke områder, øyeblikksbilder istedenfor kontinuerlig monitorering, avstå fra behandling av spesifikke opplysninger og så videre)



Slike tiltak kan typisk være:



Spesifikke sikkerhetstiltak som angår personopplysninger som skal behandles

- For eksempel:
 - kryptering
 - anonymisering
 - tilgangskontroll
 - sporbarhet



Slike tiltak kan typisk være:



Generelle sikkerhetstiltak som iverksettes på systemet hvor behandlingen utføres

- For eksempel:
 - operativ sikkerhet
 - backup
 - sikkerhet på hardware
 - teknisk og fysisk sikring



Slike tiltak kan typisk være:



Organisatoriske tiltak (styring),

- For eksempel:
 - rutiner
 - prosjektledelse
 - personellhåndtering og opplæring
 - håndtering av hendelser og brudd
 - forhold til tredjeparter



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 personvernforenne for eksempel logging og sperring av tilgang eller sperring av informasjon	Gjennomført en vurdering av personvernkonsekvenser for den registrertes rettigheter og friheter. Se matriser i punkt VI.1.2
2.	Ut fra tiltakene, vurder om:	
a.	sikringen av vernet av personopplysninger er tilstrekkelig	Ja, er ivaretatt
b.	de registrertes og andre berørte personers rettigheter og berettigede interesser er hensyntatt	Ja, er ivaretatt
c.	identifiserte risikoer er håndtert og akseptable	Ja, er ivaretatt
d.	det er restrisiko etter alle planlagte tiltak	Ja, er ivaretatt



Arbeidsoppgave fase 3



- 1. Risiko:** Gjennomføre en vurdering av personvernkonsekvenser for den registrertes rettigheter og friheter.
- 2. Tiltak:** Planlagte tiltak for å håndtere risikoene

Stikkord:

Ros analyse – fase 1 og 2



Forløp/prosess



Veileder fra
Datatilsynet

Sjekkliste fra
Datatilsynet

Behandlings
protokoll

Mal for DPIA

Mal for
Ros analyse

Rettslig
grunnlag

Personvern
prinsipper

Den
registrertes
rettigheter
og friheter

ROS- analyse
med
utgangspunkt i
den registrertes
rettigheter og
frierheter



Fase 4



Ledelsen validering av DPIA

Sammenstilling og presentasjon av funn

- Hensynet til interessenter
- Gjennomgang, beslutning og godkjenning

Del VII. Involvering av personvernombudet

Del VIII. Ledelsens godkjenning og forhåndsdrøftelse med Datatilsynet



Del VII. Involvering av personvernombudet

Personvernombudet har vært involvert gjennom hele arbeidsprosessen for gjennomføringen av denne DPIA/personvernkonsekvensvurderingen. Involveringen har bestått av rådgivning i forbindelse med forberedelse av prosessen, deltakelse i alle arbeidsmøter og fasilitering av risikoanalyse rundt de registrertes rettigheter og friheter (se kap. VI).

Vurdering fra personvernombudet

Ifølge Datatilsynet er en vurdering av personvernkonsekvenser (DPIA) en prosess som skal beskrive behandlingen av personopplysninger, og vurdere om den er nødvendig og proporsjonal. Den skal også bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastlegge risikoreduserende tiltak. Datatilsynet presiserer videre at en DPIA skal gjennomføres før en behandling av personopplysninger som innebærer høy risiko for den registrertes rettigheter og friheter settes i gang og at det å gjennomføre en DPIA ikke reparerer en ulovlig behandling av personopplysninger.

Alle tre kommunene som deltar i arbeidsgruppen for denne DPIA-prosessen har tatt i bruk digitalt tilsyn før DPIA er gjennomført. Det har vært en bevissthet i arbeidsgruppa og prosjektledelsen om at det er «bedre sent enn aldri», og personvernombudet har støttet dette. Fordi disse kommunene står midt i en prosess med kommunesammenslåing representerer DPIA-prosessen en god anledning til å revidere og kontrollere avtaler, praksis og prosedyrer, noe som også har blitt fulgt opp. Personvernombudet ser derfor ingen fare for at dette har blitt en skinnprosess, men tvert imot en reell risikovurdering som base for forbedring og tiltak forankret i nytt regelverk og faktisk praksis. Dette inntrykket ble også bekreftet i veiledningsmøte med Normsekretariatet, hvor sekretariatsmedlemmene var tydelige på at gjennomføringer av DPIA er nybrottsarbeid og ønsket innspill fra prosjektgruppa for å kunne bruke dette videre i utviklingen av sitt veiledningsmateriale.

Til tross for at prosessen viste seg å være langt mer omfattende enn noen av oss hadde forutsett før første møte, møtte jeg som personvernombud en lydhør og lærevillig prosjektledelse og arbeidsgruppe. Arbeidet bar preg av noe famling i begynnelsen, også fra personvernombudet, men det ble satt av rom til læring, diskusjoner og faglige innspill for å skape et best mulig forståelsesgrunnlag for alle parter.

Kameraovervåking i et privat hjem representerer en sterk inngripen i privatlivets fred. Personvernombudet vurderer likevel at alle identifiserte risikoer for de registrertes rettigheter og friheter vil tas ned på et akseptabelt nivå ved gjennomføring av de risikoreduserende tiltak som er beskrevet i denne rapporten. Samlet sett kan man i tillegg argumentere for at (fortsatt) gjennomføring av digitalt tilsyn vil styrke de registrertes rettigheter og friheter. Grunnen til dette er den grundige revisjonen som nå er gjort og at det digitale tilsynet, dersom alle tiltak blir fulgt opp, vil representerer en lavere inngripen i de registrertes privatliv enn dagens praksis med fysiske tilsyn.

Bakgrunn/kilde



- Veileder fra Datatilsynet:
 - <https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/vurdering-av-personvernkonsekvenser/>
- Sjekkliste fra datatilsynet:
<https://www.datatilsynet.no/globalassets/global/regelverk/veiledere/dpia-veileder/sjekkliste-for-dpiafaser.pdf>
- Normen:
 - <https://ehelse.no/Documents/Normen/Publisering/Normen%205.3.pdf>
 - s 21 kap 3.4

