Hvorfor skal vi risikovurdere?

Guro C Gidske

Personvernombud for DDV-kommunene:

Lindesnes, Mandal, Marnardal, Åseral, Hægebostad, Kvinesdal, Farsund og Flekkefjord

Hva skal jeg snakke om?

- Rollen som personvernombud
- Vurdering av personvernkonsekvenser
- DPIA
- Behandlingsprotokoll
- Tips til fremgangsmåte

Personvern er en menneskerett

- Nedfelt i FNs konvensjoner om sivile, politiske, sosiale og kulturelle rettigheter.
- Den europeiske menneskerettskonvensjonen (EMK)
- Grunnloven § 102
- Ny personopplysningslov (GDPR) fra 20.juli 2018

«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.»

- EMK artikkel 8

«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller.

Statens myndigheter skal sikre et vern om den personlige integritet.»

- Grunnloven § 102

Personvernombudet skal:

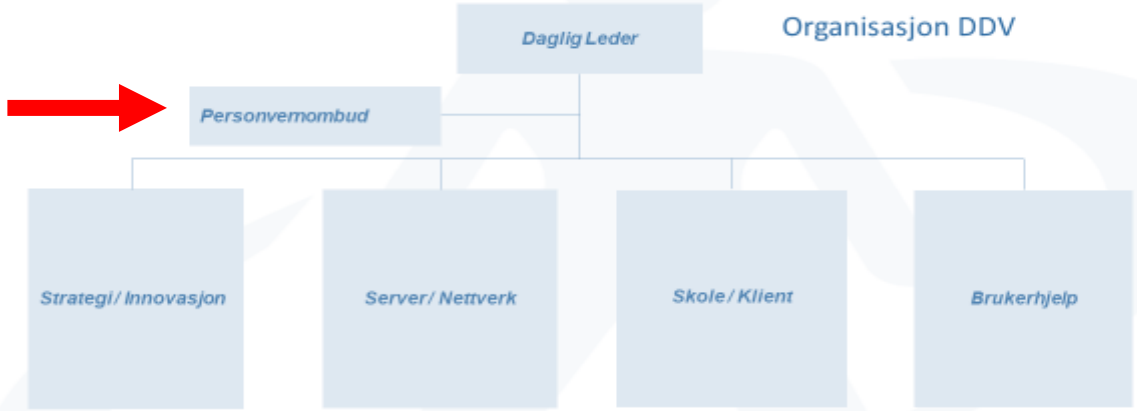
- Være fritt og uavhengig
- Informere og gi råd

Være en ressursperson for kommunen gjennom å:

- Kontrollere overholdelse av personvernregelverk
- Gi råd om vurdering av personvernkonsekvenser
- Samarbeide med og være kontaktpunkt for Datatilsynet

Hvem eier personvernombudet i DDV?

- Spleiselag mellom DDV-kommunene og plassert i DDV
- Uavhengig rolle – ingen som har instruksjonsmyndighet
- Ca 50 000 innbyggere/registrerte



Hvordan risikovurdere personvern?

- Risikovurdering (identifisert trussel + sannsynlighet x konsekvens)
- som tar utgangspunkt i de registrertes rettigheter og friheter
- Informasjonssikkerhet er en del av dette bildet

Vurdering av personvernkonsekvenser / DPIA

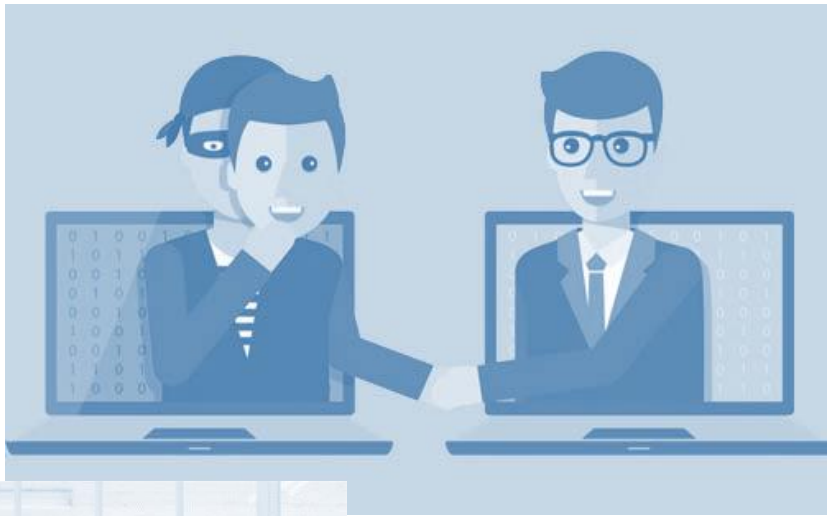
- Skal sikre at personvernet til de som er registrert i løsningen ivaretas
- Plikt etter Artikkel 35 i den nye personopplysnings-forordningen (GDPR)
- En prosess som skal beskrive behandlingen av personopplysninger, og vurdere om den er *nødvendig og proporsjonal*

Personvernkonsekvensvurdering / DPIA er et verktøy

- Alle har plikt til å ha en oversikt over behandlinger av personopplysninger som foretas i virksomheten som del av interkontrollen sin.
- Å gjennomføre en DPIA reparerer ikke en ulovlig behandling av personopplysninger, MEN:
- Vurderingen skal være et verktøy til bruk i beslutningsprosesser som gjelder behandlingen

Tradisjonell risiko- og sårbarhetsanalyse (ROS) vs personvernkonsekvensanalyse/DPIA

- **ROS** kan forankres i Artikkel 32 om sikkerhet ved behandlingen (av personopplysninger)
- Fokuserer gjerne på personopplysnings*sikkerhet*
- Sannsynlighet for og konsekvens av *at* det oppstår hendelser
- Ansvar: Behandlingsansvarlig og databehandler
- Trussel kan «fikses» med penger - løses teknisk/organisatorisk



- **DPIA** forankres i Artikkel 35 om vurdering av personvernkonsekvenser
- Vurderer konsekvenser for personvernet til den enkelte registrerte dersom (når?) det oppstår hendelser
- Ansvar: Behandlingsansvarlig
- Konsekvenser kan ikke fikses med penger

Eksempler på mulige konsekvenser for de registrerte

At den registrerte:

- ikke har mulighet til å utøve sine rettigheter
- ikke får tilgang til tjenester eller muligheter
- har manglende kontroll over bruken av personopplysninger
- utsettes for diskriminering
- utsettes for id-tyveri, svindel, økonomiske tap, tap av omdømme, fysisk skade, tap av konfidensialitet, reidentifisering av pseudonymiserte data
- eller annen betydelig økonomisk eller sosial ulempe.

Må man alltid gjennomføre en DPIA?

- **Vurdering av personvernkonsekvenser** er en prosess som uansett skal gjennomføres for **alle behandlinger**.
- DPIA gjentar denne prosessen, men da først og fremst for å finne de **ekstra tiltak**ene som må til for å redusere en ***høy risiko*** som man ikke har klart å redusere tidligere.

Altså:

Vurdering av personvernkonsekvens = høy risiko

Høy risiko + risikoreduserende tiltak = *fortsatt høy risiko* = DPIA

MEN: DPIA skal likevel uansett gjennomføres dersom to av disse kriteriene er til stede

- Evaluering eller poengvurdering (scoring)
- Automatiserte avgjørelser
- Systematisk overvåkning (screening)
- Sensitive personopplysninger
- Behandling av personopplysninger i stor skala
- To eller flere datasett som sammenstilles
- Personopplysninger om registrerte med særskilt beskyttelsesbehov
- Bruk av ny teknologi eller eksisterende teknologi som brukes til nye formål
- Personopplysninger overføres til utlandet
- Kontekst begrenser muligheten for de registrerte til å utøve sine rettigheter

Digitalt tilsyn innebærer for eksempel:

- Evaluering eller poengvurdering (scoring)
- Automatiserte avgjørelser
- Systematisk overvåkning (screening)
- Sensitive personopplysninger
- Behandling av personopplysninger i stor skala
- To eller flere datasett som sammenstilles
- Personopplysninger om registrerte med særskilt beskyttelsesbehov
- Bruk av ny teknologi eller eksisterende teknologi som brukes til nye formål
- Personopplysninger overføres til utlandet
- Kontekst begrenser muligheten for de registrerte til å utøve sine rettigheter

Hvordan defineres høy risiko?

Momenter i vurderingen av om en behandling av personopplysninger utgjør en høy risiko er følgende:

- behandlingens art
- behandlingens omfang
- behandlingens formål
- sammenhengen behandlingen utføres i (kontekst)

Visse typer behandling av personopplysninger innebærer en mer alvorlig inngripen i personvernet enn andre fordi:

- Personopplysningene som behandles er av en **særskilt sensitiv** karakter.
- Måten personopplysningene behandles på utgjør et **særskilt inngrep** i de registrertes rettigheter og friheter.

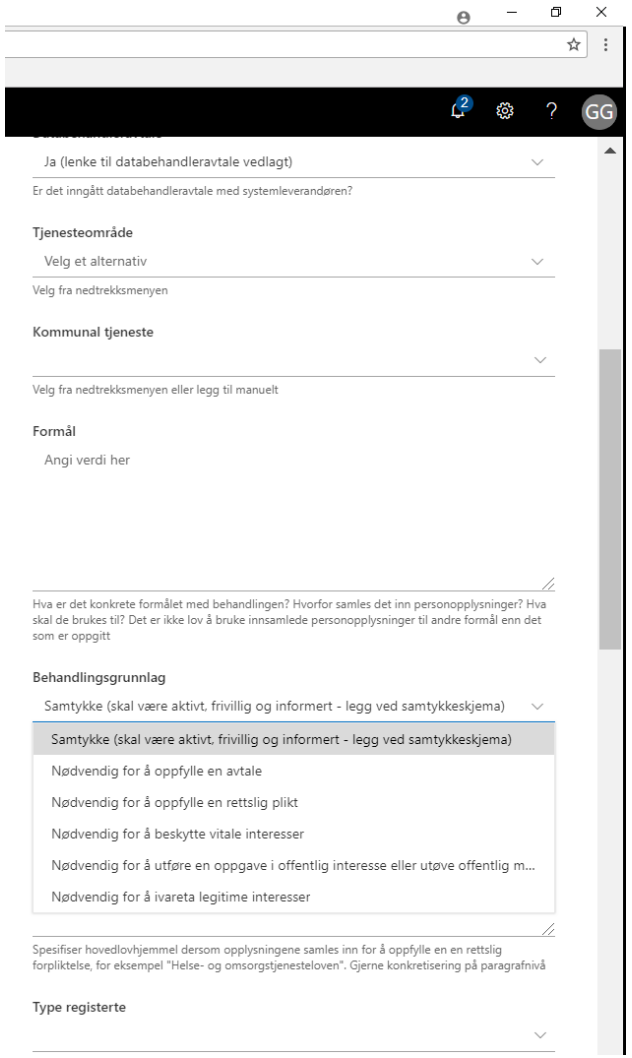
Mye av denne bakgrunnsinformasjonen finnes i Behandlingsprotokollen

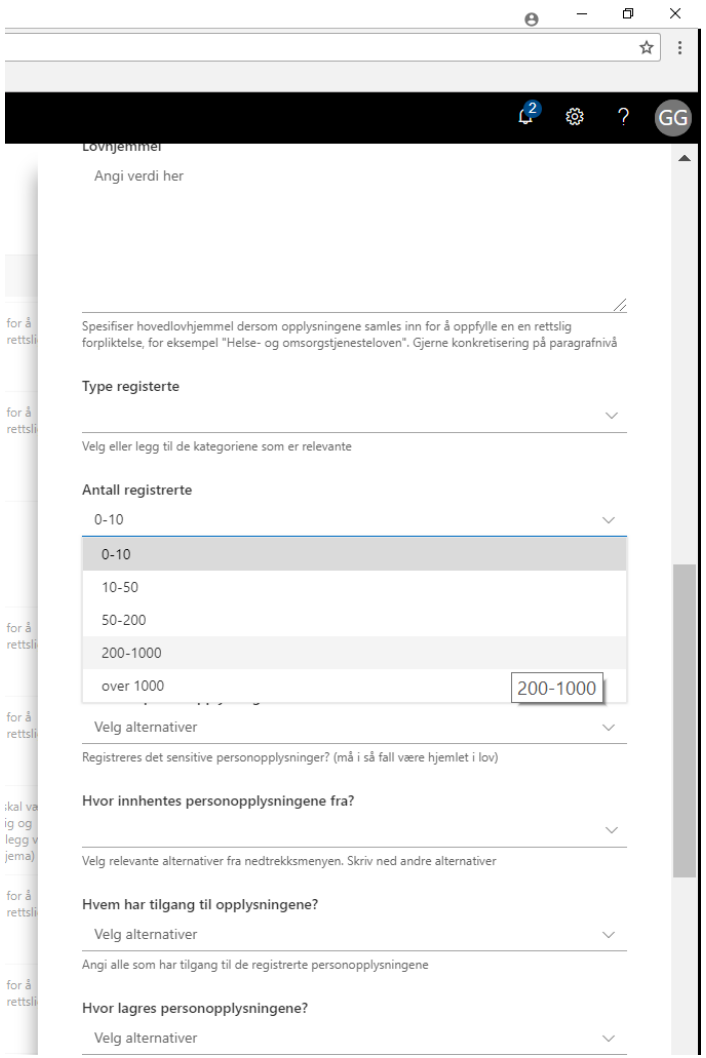
- Alle virksomheter som behandler personopplysninger, skal føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar.
- Informasjonen som ligger i behandlingsprotokollen skal også reflekteres i databehandleravtalene
- Dersom protokollen er god, vil den også kunne danne utgangspunkt for innsynshenvendelser, DPIA og personvernerklæringer

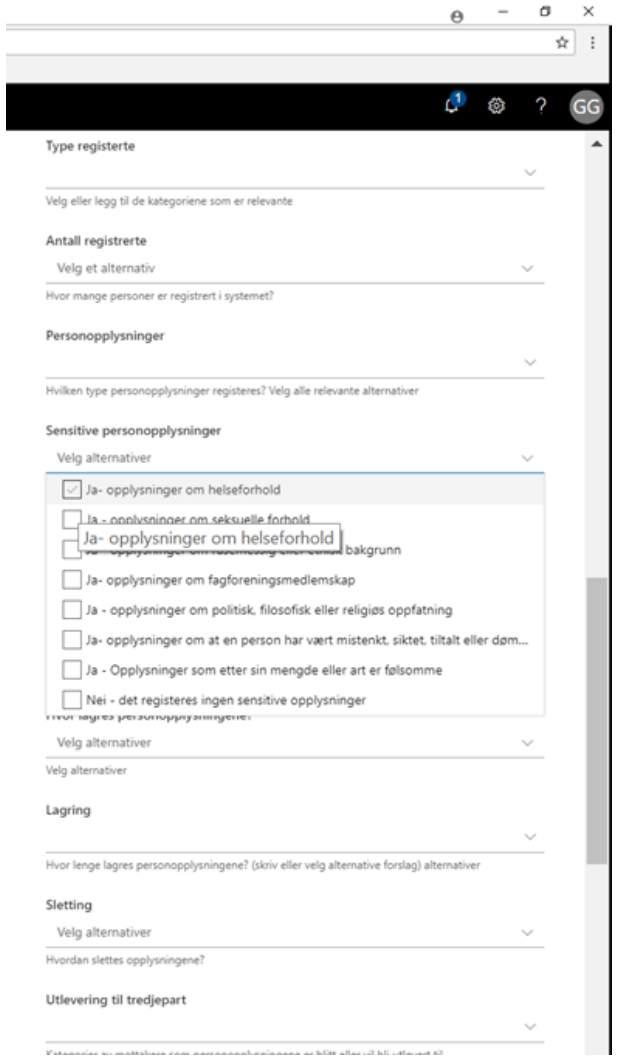
Behandlingsprotokoll i DDV-kommunene

- Hensikt: Opprette en felles protokollbase over gjennomgående behandlingsaktiviteter for alle DDV-kommunene
- Hvordan: Protokoll føres i en mal i SharePoint opprettet for dette formålet
- Informasjonssikkerhetsansvarlige i kommunene registrerer behandlinger i samarbeid med sine fagkontakter
- Ca 150 behandlinger registrert hittil, fordelt på alle fagområder

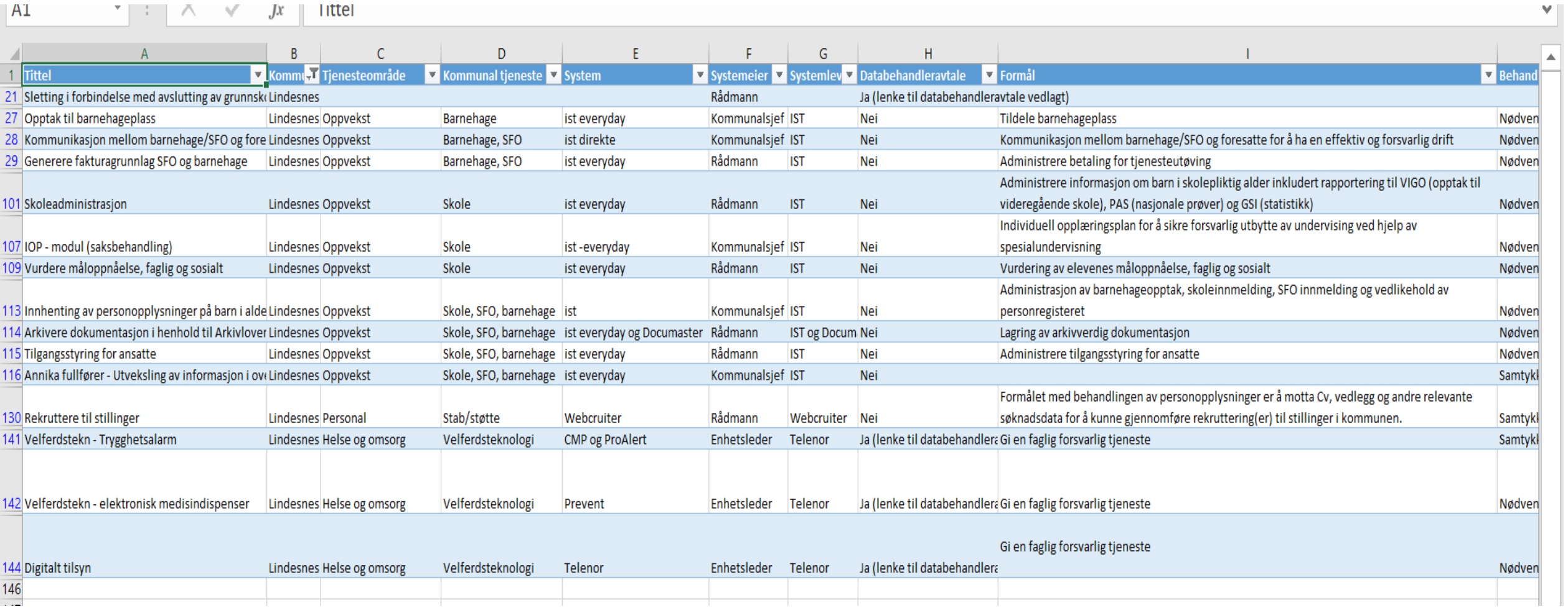
Eksempler på registreringsfelt







Skjermdump – Behandlingsprotokoll, rapport



A1 | Tittel

	A	B	C	D	E	F	G	H	I	
1	Tittel	Kommu	Tjenesteområde	Kommunal tjeneste	System	Systemeier	Systemlev	Databehandleravtale	Formål	Behand
21	Sletting i forbindelse med avslutting av grunnsk	Lindesnes				Rådmann		Ja (lenke til databehandleravtale vedlagt)		
27	Opptak til barnehageplass	Lindesnes	Oppvekst	Barnehage	ist everyday	Kommunalsjef	IST	Nei	Tildele barnehageplass	Nødven
28	Kommunikasjon mellom barnehage/SFO og fore	Lindesnes	Oppvekst	Barnehage, SFO	ist direkte	Kommunalsjef	IST	Nei	Kommunikasjon mellom barnehage/SFO og foresatte for å ha en effektiv og forsvarlig drift	Nødven
29	Generere fakturagrunnlag SFO og barnehage	Lindesnes	Oppvekst	Barnehage, SFO	ist everyday	Rådmann	IST	Nei	Administrere betaling for tjenesteutøving	Nødven
101	Skoleadministrasjon	Lindesnes	Oppvekst	Skole	ist everyday	Rådmann	IST	Nei	Administrere informasjon om barn i skolepliktig alder inkludert rapportering til VIGO (opptak til videregående skole), PAS (nasjonale prøver) og GSI (statistikk)	Nødven
107	IOP - modul (saksbehandling)	Lindesnes	Oppvekst	Skole	ist -everyday	Kommunalsjef	IST	Nei	Individuell opplæringsplan for å sikre forsvarlig utbytte av undervising ved hjelp av spesialundervisning	Nødven
109	Vurdere måloppnåelse, faglig og sosialt	Lindesnes	Oppvekst	Skole	ist everyday	Rådmann	IST	Nei	Vurdering av elevenes måloppnåelse, faglig og sosialt	Nødven
113	Innhenting av personopplysninger på barn i alde	Lindesnes	Oppvekst	Skole, SFO, barnehage	ist	Kommunalsjef	IST	Nei	Administrasjon av barnehageopptak, skoleinnmelding, SFO innmelding og vedlikehold av personregisteret	Nødven
114	Arkivere dokumentasjon i henhold til Arkivlover	Lindesnes	Oppvekst	Skole, SFO, barnehage	ist everyday og Documaster	Rådmann	IST og Docum	Nei	Lagring av arkivverdig dokumentasjon	Nødven
115	Tilgangsstyring for ansatte	Lindesnes	Oppvekst	Skole, SFO, barnehage	ist everyday	Rådmann	IST	Nei	Administrere tilgangsstyring for ansatte	Nødven
116	Annika fullfører - Utveksling av informasjon i ov	Lindesnes	Oppvekst	Skole, SFO, barnehage	ist everyday	Kommunalsjef	IST	Nei		Samtykk
130	Rekruttere til stillinger	Lindesnes	Personal	Stab/støtte	Webcruiter	Rådmann	Webcruiter	Nei	Formålet med behandlingen av personopplysninger er å motta Cv, vedlegg og andre relevante søknadsdata for å kunne gjennomføre rekruttering(er) til stillinger i kommunen.	Samtykk
141	Velferdstekn - Trygghetsalarm	Lindesnes	Helse og omsorg	Velferdsteknologi	CMP og ProAlert	Enhetsleder	Telenor	Ja (lenke til databehandlera	Gi en faglig forsvarlig tjeneste	Samtykk
142	Velferdstekn - elektronisk medisindispenser	Lindesnes	Helse og omsorg	Velferdsteknologi	Prevent	Enhetsleder	Telenor	Ja (lenke til databehandlera	Gi en faglig forsvarlig tjeneste	Nødven
144	Digitalt tilsyn	Lindesnes	Helse og omsorg	Velferdsteknologi	Telenor	Enhetsleder	Telenor	Ja (lenke til databehandlera	Gi en faglig forsvarlig tjeneste	Nødven
146										

	N	O	P	Q	R	S	
1	Personopplysninger	Sensitive personopplysninger	Hvor innhentes personopplysningene fra?	Hvor lagres pers	Hvem har tilgang til opplysningen	Personvernkonsekvensutredning (DF	ROS-analyse
21							
27	Navn;#Adresse;#Telefonnummer;#E-postadresse;#Fødselsnummer (11 siff	Nei - det registeres ingen sensitive opplysninger	Den registrerte;#Fagsystem	I fagsystemet	Brukere med spesiell tilgang	DPIA er ikke gjennomført	ROS-analyse er ikke
28	Navn;#Adresse;#Telefonnummer;#E-postadresse;#Fødselsnummer (11 siff	Ja- opplysninger om helseforhold;#Ja - Opplysninger som ett	Den registrerte;#Pårørende;#Fagsystem;#Skole	I fagsystemet	Brukere med spesiell tilgang	DPIA er ikke gjennomført	ROS-analyse er ikke
29	Navn;#Fødselsnummer (11 siffer)	Nei - det registeres ingen sensitive opplysninger	Fagsystem	I fagsystemet	Alle brukere av systemet	DPIA er ikke gjennomført	ROS-analyse er ikke
101	Navn;#Adresse;#Telefonnummer;#E-postadresse;#Fødselsnummer (11 siff	Ja- opplysninger om helseforhold	Den registrerte;#Fagsystem;#Skole/Barnehage	I fagsystemet	Brukere med spesiell tilgang	DPIA er ikke gjennomført	ROS-analyse er gjenn
107	Navn;#Adresse;#Telefonnummer;#Fødselsdato (6 siffer);#Helseopplysning	Ja- opplysninger om helseforhold;#Ja - Opplysninger som ett	Den registrerte;#Fagsystem;#Fastlege/Spesiali	I kommunens arkiv	Brukere med spesiell tilgang	DPIA er ikke gjennomført	ROS-analyse er ikke
109	Navn;#Fødselsdato (6 siffer);#Karakterer/vurderinger	Nei - det registeres ingen sensitive opplysninger	Fagsystem	I fagsystemet;#I ko	Alle brukere av systemet	DPIA er ikke gjennomført	ROS-analyse er ikke
113	Navn;#Adresse;#Fødselsnummer (11 siffer);#Kjønn;#Statsborgerskap;#Ekte	Nei - det registeres ingen sensitive opplysninger	Folkeregister	I fagsystemet	Brukere med spesiell tilgang	DPIA er ikke gjennomført	ROS-analyse er ikke
114	Navn;#Adresse;#Telefonnummer;#E-postadresse;#Fødselsnummer (11 siff	Ja- opplysninger om helseforhold	Fagsystem	I kommunens arkiv	Brukere med spesiell tilgang	DPIA er ikke gjennomført	ROS-analyse er ikke
115	Navn;#Telefonnummer;#E-postadresse;#Fødselsnummer (11 siffer)	Nei - det registeres ingen sensitive opplysninger	Den registrerte;#Fagsystem	I fagsystemet	Brukere med spesiell tilgang	DPIA er ikke gjennomført	ROS-analyse er ikke
116							
130	Navn;#Adresse;#Telefonnummer;#Fødselsdato (6 siffer);#E-postadresse;#k	Nei - det registeres ingen sensitive opplysninger	Den registrerte	I fagsystemet;#I ko	Brukere med spesiell tilgang	DPIA er ikke gjennomført	ROS-analyse er ikke
141	Navn;#Adresse;#Telefonnummer;#Fødselsdato (6 siffer);#D-nummer;#Ekte	Ja- opplysninger om helseforhold	Den registrerte;#Pårørende;#Fagsystem	I fagsystemet	Brukere med spesiell tilgang	DPIA er ikke gjennomført	ROS-analyse er gjenn
142	Navn;#Adresse;#Telefonnummer;#Fødselsdato (6 siffer);#Helseopplysning	Ja- opplysninger om helseforhold	Den registrerte;#Pårørende;#Fastlege	I fagsystemet	Brukere med spesiell tilgang	DPIA er ikke gjennomført	ROS-analyse er gjenn
144	Navn;#Biometri (ansiktsform, stemme, fingeravtrykk etc)	Ja - Opplysninger som etter sin mengde eller art er følsomm	Den registrerte;#Pårørende;#Fagsystem	I fagsystemet	Brukere med spesiell tilgang	DPIA er gjennomført - akseptabel risiko	ROS-analyse er gjenn
146							
147							

Tips til fremgangsmåte - DPIA

- Få **kontroll på formålet** med behandlingen
- **Skaff oversikt** over alle personopplysninger som behandles
- Få oversikt over **flyten av informasjon** mellom systemene – både internt og eksternt (visualiser eller bruk tabell)
- **Vurder utfordringer** knyttet til behandling av personopplysninger ved alle punkter i flytoversikten
- Løft blikket og **vurder helheten** av behandlinger opp mot formålet. Er det mulig å begrense behandlingen på enkelte områder?
- **Tenk dataminimering**.

Hvem skal delta ved gjennomføring av DPIA?

- Behandlingsansvarlig (kommunen)
- Databehandler (systemleverandør)
- Personvernombud
- Representant for de registrerte

I større prosjekter bør man sette av god tid til dette, viktig at bakgrunnsinformasjon og dokumentasjon er på plass

Lykke til!