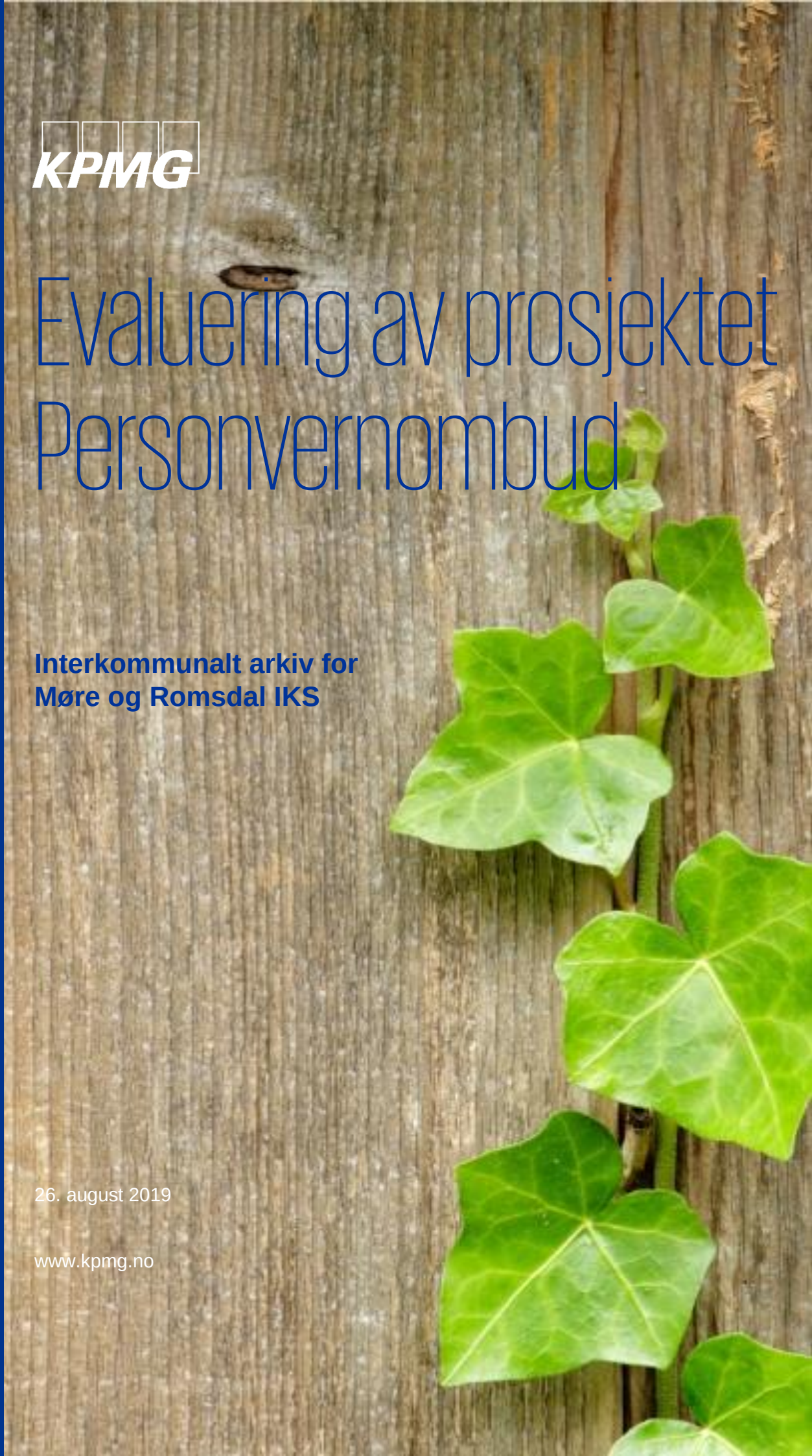

Evaluering av prosjektet Personvernombud

Interkommunalt arkiv for Møre og Romsdal IKS

26. august 2019

www.kpmg.no

Forord

For å etterleve nye personvernkrav, etablerte Interkommunalt arkiv for Møre og Romsdal IKS (IKA MR) i 2018 prosjektet *Personvernombud*. Prosjektet leverer tjenesten personvernombud til 26 av eierkommunene, samt til Møre og Romsdal fylkeskommune. Tjenestene leveres basert på en prosjektavtale med varighet til 31.12.2020, mellom IKA MR og eierkommunene som har inngått avtale om kjøp av slike tjenester fra IKA MR. Ved opprettelsen av prosjektet ble det besluttet at ordningen skulle evalueres i 2019, og IKA MR har derfor etter en anbudsprosess bedt KPMG gjøre en slik evaluering.

Denne rapporten vurderer om den etablerte ordningen ivaretar de lovpålagte kravene til personvernombud på en faglig forsvarlig og effektiv måte for eierkommunene. Rapporten oppsummerer også erfaringer som representanter for et utvalg prosjektdeltakere har gjort seg med ordningen. Evalueringen skal danne et grunnlag for styret i IKA MR, samt for beslutningstakere i eierkommunene, ved vurdering om, og eventuelt på hvilken form, avtalen skal videreføres.

Oppbygging av rapporten

Kapittel 1 er innledning til rapporten. Her blir formål, problemstillinger og metode presentert. I kapittel 2 svarer vi på de problemstillingene som skal danne grunnlaget for vår evaluering av prosjektet personvernombud, mens våre anbefalinger fremgår av kapittel 3. Eksterne evalueringskriterier fremgår i kortfattet form av kapittel 4 – vedlegg.

Tekst som er gjengitt fra eksterne kilder er satt i kursiv.

Hovedbudskap

Prosjektet Personvernombud har pågått i overkant av et år. Personvernombudene og prosjektdeltakerne beskriver et åpent og godt samarbeid for å etablere nødvendig personvernrammeverk, og ellers legge til rette for etterlevelse av lovkrav. Det er vår vurdering at personvernombudene i IKA MR har tilstrekkelig fagkompetanse, og gjør et viktig arbeid for å bidra til å løfte prosjektdeltakerne på personvernområdet. Ordningen legger til rette for et tett samarbeid mellom to personvernombud om å levere slike tjenester. Dette er gunstig både fordi det reduserer sårbarheten ved fravær og ved skifte av personvernombud, og fordi det lar personvernombudene være en del av et lite miljø, i motsetning til – som i mange virksomheter - der det er ett personvernombud som er alene om rollen, og som gjerne også ivaretar den kun som en andel av stillingen sin.

Det er liten grad av dokumentasjon i prosjektet. Eksempelvis foreligger det ikke et klart mandat for prosjektet, med en handlingsplan med milepæler som viser planlagte leveranser fra personvernombudene og prosjektdeltakerne, en oversikt over hvilke beslutninger som skal eskaleres til hvilket nivå hos hhv. IKA MR og prosjektdeltakerne osv. Til tross for begrenset grad av styring av prosjektet, har ombudene klart å levere tjenester som prosjektdeltakerne har vært godt fornøyd med så langt i prosjektet. På et overordnet nivå er det beskrevet hvilke oppgaver personvernombudet skal levere til prosjektdeltakerne. Det er likevel en risiko for at oppgaver "faller mellom to stoler" ved at enkelte prosjektdeltakere kan forvente at ombudet tar et større ansvar for deres etterlevelse enn det som ligger i ombudsrollen slik IKA MR tolker den. Personvernombudene og kontaktpersonene hos prosjektdeltakerne er relativt samstemte om hva som er hhv. ombudets og virksomhetens rolle og ansvar for etterlevelse av krav i personvernlovgivningen. Rolle- og ansvarsfordelingen virker imidlertid ikke å være like tydelig for ledelsen hos alle prosjektdeltakerne.

Personvernombudene har ikke opplevd at deres uavhengighet har blitt utfordret ved at de har blitt forsøkt påvirket til å innta et bestemt standpunkt. I situasjoner der ledelsen i virksomheten ikke velger å følge ombudets råd, dokumenterer ombudet sine vurderinger. Hos en del prosjektdeltakere virker det å være "en

lang vei" fra ombudet til øverste leder, det er krevende for ombudet å få innpass i ledergruppen, og det kan stilles spørsmål ved om ombudet i praksis rapporterer til virksomhetens øverste leder.

Begge personvernombudene har relevant utdanning og dybdeforståelse for personopplysningsloven (POL). De forteller at de har en interesse for informasjonsteknologi, og oppleves av prosjektdeltakerne til å ha tilfredsstillende forståelse for informasjonsteknologi og datasikkerhet. Ombudene har gjennom vel et års erfaring opparbeidet seg en relativt god forståelse for virksomheten, derunder for de behandlings-aktivitetene som utføres. Ombudene oppleves å ha en genuin interesse for personvern, og for at prosjektdeltakerne skal utvikle en økt modenhet på området.

Prosjektdeltakerne beskriver ombudet som en god støttespiller og diskusjonspartner som de bruker aktivt ved personvernrelaterte problemstillinger. Ombudene er på sin side opptatt av å være tilgjengelige som rådgivere ved behov. Ombudet involveres ved viktige personvernrelaterte vurderinger, derunder ved avvik. Ingen av prosjektdeltakerne har fullført en personvernkonsekvensvurdering, men ombudet har vært involvert i tidlig fase av flere slike vurderinger.

Personvernombud er pålagt å følge opp en rekke oppgaver iht. personopplysningsloven. Innledningsvis i prosjektet har ombudenes hovedfokus vært å rådgi og støtte prosjektdeltakerne i deres arbeid. Begge parter har opplevd det som helt nødvendig, men er også enige om at det nå er på tide med økt fokus på kontroll for å sikre at prosjektdeltakerne gjennomfører sine plikter i samsvar med personopplysningsloven. Både ombudene og prosjektdeltakerne legger til grunn at de blir fulgt opp "godt nok" i dag, og beskriver en situasjon der ombudene svarer raskt på alle innkommende henvendelser, med godt begrunnete svar.

Personvernombudene har ikke utført en systematisk risikovurdering av personvernrisiko hos den enkelte prosjektdeltaker, og har heller ikke etablert en risikobasert handlingsplan over hvilke kontroller som skal utføres hos den enkelte virksomhet.

De to personvernombudene er ombud for hhv. 13 og 14 prosjektdeltakere, hvilket gjør at de i snitt har om lag 7% av en full stilling til oppfølging av ombudsrollen hos den enkelte prosjektdeltaker. I praksis har de imidlertid mindre tid per virksomhet, som følge av at det også medgår tid til administrasjon, kompetanseheving, reisevirksomhet m.v. Representanter for begge parter stiller spørsmål ved om prosjektet har tilstrekkelig ressurser når ombudene i større grad skal utføre kontroller. Flere kommuner skal imidlertid slå seg sammen 1. januar 2020, og antall prosjektdeltakere vil da reduseres fra 27 til 19. Dette vil bidra til at personvernombudet får mer tid tilgjengelig per prosjektdeltaker.

Flere prosjektdeltakere forteller at de har nytte av samhandlingsplattformen Teams i prosjektet. Enkelte er imidlertid ikke klar over at dette er tatt i bruk i prosjektet, og ombudene når dermed ikke ut til alle prosjektdeltakerne med informasjonen som deles der. Det er ikke tydeliggjort hvilke kanaler prosjektdeltakerne kan benytte for å gi tilbakemeldinger på arbeidet som gjøres i prosjektet.

Basert på tilgjengelig informasjon, er det vår vurdering at personvernombudene gjør en god innsats for å bidra til økt etterlevelse blant prosjektdeltakerne, og at ombudene i stor grad etterlever lovkrav til innhold i deres rolle. På enkelte områder stiller vi spørsmål ved hvorvidt lovkravene oppfylles fullt ut, herunder:

- Rapportering til øverste leder. Det er indikasjoner på at ombudet i praksis ikke rapporterer til virksomhetens øverste leder hos enkelte av prosjektdeltakerne (POL Artikkel 38 (3)).
- Kapasitet. Det vurderes som sannsynlig at personvernombudet pt. ikke har tilstrekkelig tid til å gjennomføre alle sine forpliktelser iht. regelverket på betryggende vis (POL Artikkel 38 (2))
- Risikovurdering. Personvernombudene har ikke i tilstrekkelig grad vurdert risikoen som er forbundet med behandlingsaktivitetene prosjektdeltakerne utfører. (POL Artikkel 39 (2))
- Etterleveseskontroll. Ombudet utfører i begrenset grad kontroll av virksomhetens etterlevelse av personopplysningsloven (POL Artikkel 39 (1, b))

Anbefalte justeringer av prosjektet Personvernombud

Selv om det gjøres mye godt arbeidet i prosjektet, foreslås noen justeringer for å legge til rette for økt grad av etterlevelse av regelverket og en enda mer effektivt arbeidform (se rapportens kapittel 3 for en utdypning av den enkelte anbefaling):

I. Tydeliggjøring av prosjektets mandat

Det er behov for å tydeliggjøre et mandat for personvernombudene. Dette bør gjøres både for å sikre at personvernombudene har en helhetlig og enhetlig tilnærming til arbeidet i tråd med lovkrav, for å bidra til å skape trygge rammer for arbeidet de skal gjøre, samt for å tydeliggjøre krav og forventninger overfor prosjektdeltakerne.

II. Tydeliggjørring av viktige strukturer i prosjektet

Det er behov for å tydeliggjøre viktige strukturer og samhandlingsarenaer i prosjektet, for å legge til rette for et mer forutsigbart og effektivt samarbeid mellom personvernombudet og den enkelte prosjektdeltaker.

III. Risikovurdering og utførelse av kontroller

Personvernombudet bør gjøre en helhetlig vurdering av hvilke utfordringer og risikoer prosjektdeltakerne har for oppfyllelse av kravene i personopplysningsloven. Basert på en slik vurdering, bør det etableres en handlingsplan med oversikt over hvilke kontroller som skal utføres når. En slik tilnærming legger til rette for effektiv ressursbruk, samt for overholdelse av lovkrav.

IV. Vurdering av ressursbehov

Det bør gjøres en vurdering av om prosjektet har tilstrekkelig ressurser til at personvernombudene kan ivareta alle sine oppgaver iht. lovkrav og prosjektavtalen på en betryggende måte.

Innhold

1. Innledning

1.1 Formål og avgrensning

Formålet med oppdraget er å evaluere prosjektet Personvernombud i IKA MR.

Oppdraget er praktisk rettet, og sluttrapporten skal veilede beslutningstakere i IKA MR og prosjektdeltakerne med hensyn til hvilke tilpasninger som eventuelt bør gjøres, for å legge til rette for et effektivt og forsvarlig tjenestetilbud.

Det har ikke vært et formål å vurdere i hvilken grad eierkommunene og Fylkeskommunen som inngår i samarbeidet (heretter *prosjektdeltakerne*) etterlever kravene i personvernlovgivningen. Det er gjort enkelte observasjoner av prosjektdeltakeres arbeid for å etterleve personvernkrav. Dette er gjort med formål om å få en bedre forståelse av sentrale rammebetingelser for prosjektet Personvernombud, og gir ikke et grunnlag for å vurdere i hvilken grad den enkelte prosjektdeltaker etterlever regelverket, eller deres modenhet på området.

1.2 Problemstillinger

Evalueringen har søkt å belyse i hvilken grad personvernombudet ivaretar sine forpliktelser som personvernombud. I denne forbindelse har vi vurdert ulike problemstillinger, herunder:

1. Har personvernombudet en tilstrekkelig uavhengig stilling i virksomheten?
2. Har personvernombudet tilstrekkelig kompetanse om kravene i personopplysningsloven og annet relevant regelverk til å kunne ivareta kundenes behov på forsvarlig og effektivt vis?
3. Har personvernombudet tilstrekkelig forståelse for behandlingsaktiviteter, IT-systemer, informasjonssikkerhet og personvernbehovene i virksomhetene til å kunne ivareta kundenes behov på forsvarlig og effektivt vis?
4. Har personvernombudet personlige kvaliteter og kunnskap, samt en posisjon i virksomheten som gjør det i stand til å utføre oppgavene sine på forsvarlig og effektivt vis?
5. Hvilke erfaringer har IKA MR gjort seg i rollen som personvernombud for eierkommunene?
6. Hvilke erfaringer har eierkommunene gjort seg med ordningen så langt?
7. Hvilke justeringer kan / bør eventuelt gjøres i dagens avtale for å legge til rette for en forsvarlig og effektiv ivaretakelse av personvernombudsrollen på vegne av kundene?
8. Hvordan håndteres slike tjenester av andre? "Best practice" og sammenligning.

1.3 Evalueringskriterier

Observasjoner er vurdert opp mot:

- Krav i Personopplysningsloven til rollen som personvernombud
- Article 29 Data Protection Working Party's Guidelines on Data Protection Officers
- Det norske og danske datatilsynet sitt veiledningsmateriale til rollen som personvernombud
- Prosjektavtalen mellom IKA MR og prosjektdeltakerne

I tillegg har KPMG vurdert Personvernombudenes forståelse av sine forpliktelser overfor prosjektdeltakerne, opp mot eierkommunens forventninger til leveranser fra personvernombudene. Enkelte observasjoner har også blitt vurdert opp mot god praksis for prosjektstyring.

Med personopplysningsloven mener vi her den nye personopplysningsloven som trådte i kraft 20. juli 2018, og som også gjennomfører forordning EU 2016/679 (Personvernforordningen).

1.4 Metode

Evalueringen er gjennomført basert på kvalitative metoder og datainnsamling. Konkret er det benyttet en kombinasjon av semi-strukturerte dybdeintervjuer som er gjennomført 1:1, og dokumentanalyse.

Intervjuer og dokumentanalyse ble gjennomført i kartleggingsfasen av oppdraget. Metodene utfyller hverandre og sørger for at dataene har blitt triangulert og validert.

Semi-strukturerte intervjuer

Semi-strukturerte intervjuer er intervjuer som følger en intervjuguide med forhåndsdefinerte spørsmål som skal belyses, men som likevel gir en fleksibilitet til å gjennomføre intervjuet på en naturlig måte ut i fra hvordan samtalen utvikler seg.

I kartleggingsfasen ble det gjennomført intervjuer med representanter for IKA MR og for utvalgte prosjektdeltakere i samarbeidet, for å få en god oversikt over prosjektet Personvernombud, samt over hvilke erfaringer ulike deltakere i prosjektet har gjort seg så langt i samarbeidet. Følgende roller er intervjuet:

- Daglig leder for IKA MR
- Begge medarbeiderne som fyller rollen som Personvernombud i IKA MR
- Representanter for følgende prosjektdeltakere:
    - Møre og Romsdal Fylkeskommune
    - Molde Kommune
    - Ålesund Kommune
    - Fræna kommune
    - IKT-ORKidé

IKT-ORKidé er et IKT-samarbeid mellom samtlige kommuner på Nordmøre, samt romsdalskommunene Nesset og Fræna.

Prosjektdeltakerne som er intervjuet er valgt ut av KPMG, basert på innspill fra IKA MR. I tillegg til overnevnte virksomheter, var det ønskelig å intervjue ytterligere et par eierkommuner med et relativt lavt innbyggertall. Flere aktuelle intervjukandidater ble kontaktet, men ingen av dem hadde anledning til å stille opp til intervju. Vår vurdering er imidlertid at KPMG likevel har samlet inn nødvendig informasjon til å kunne evaluere prosjektet Personvernombud.

Intervjuene tok utgangspunkt i en intervjuguide som ble kvalitetssikret før gjennomføring av intervjuene. Dette sikrer at vi får belyst sentrale problemstillinger, og at vi innhenter sammenlignbar informasjon fra intervjuobjektene. Utover dette var intervjuene av mer generell karakter for at evalueringsteamet skulle kunne danne seg et bilde av hvordan prosjektet Personvernombud fungerer i praksis.

Representanter for IKA MR ble gitt anledning til å inngi innspill til intervjuguiden som ble benyttet ved intervju av representanter for prosjektdeltakerne.

Dokumentanalyse

Dokumentanalyse er en strukturert gjennomgang av eksisterende dokumentasjon, med mål om å sammenstille informasjon fra ulike kilder for å belyse aktuelle problemstillinger.

Vi gjennomgikk tilgjengelig styrende dokumentasjon for prosjektet Personvernombud, samt relevant dokumentasjon som dokumenterte hvordan prosjektet har arbeidet, hvilke erfaringer prosjektdeltakerne har gjort seg i løpet av samarbeidet m.v.

Dokumentasjon som ble gjennomgått i forbindelse med evalueringen omfatter:

- ✓ Krav om personvernombod i alle kommunar - førespurnad om fellesløysing
- ✓ Prosjektinvitasjon - felles personvernombud
- ✓ Bindende deltagelse - i prosjekt Personvernombud ved IKA Møre og Romsdal IKS
- ✓ Prosjektavtale – deltagelse i prosjekt – Personvernombud
- ✓ Rolle og oppgåver
- ✓ Forslag til DPIA-prosedyre
- ✓ Revisjonsprosedyre
- ✓ Møtereferat fra referansegruppemøte
- ✓ Eksempel på avvikshåndtering til revisjon (sensurert)
- ✓ Anbefaling fra personvernombudet vedrørende tofaktorautentifisering for innloggingsløsninger

Dokumentene ble gjennomgått for å identifisere eventuelle styringsutfordringer. Observasjoner og funn er sett opp mot teori og beste praksis. Datagrunnlaget har blitt supplert med intervjudata for å triangulere funnene, samt for å identifisere eventuelle ytterligere styringsutfordringer.

2. Vurdering av praksis

2.1 Etablering og oppfølging av prosjektet Personvernombud

2.1.1 IKA MRs styring og kontroll med prosjektet

De to personvernombudene som betjener prosjektdeltakerne i prosjektet ble ansatt i IKA MR i mai 2018. Begge var på det tidspunktet nyutdannete jurister, med spesialisering innen personvern. Det var da inngått en prosjektavtale mellom IKA MR og prosjektdeltakerne, som på et overordnet nivå stilte noen forventninger til personvernombudene.

Det fagansvarlige personvernombudet rapporterer til daglig leder for IKA MR, som har det overordnete ansvaret for prosjektet. Daglig leder har ansvaret for arkivfunksjonen på vegne av IKA MRs eiere, og har ikke tidligere erfaring fra arbeid med personvern. I forbindelse med etablering av prosjektet Personvernombud har daglig leder satt seg inn i det nye personvernregelverket på et overordnet nivå, med fokus på rollen som personvernombud.

Det foreligger en prosjektinvitasjon til eierne i IKA MR som skisserer noen overordnede rammer for prosjektet, samt en prosjektavtale inngått mellom IKA MR og de virksomhetene som valgte å inngå i prosjektet. Avtalen er kortfattet, men gir en overordnet beskrivelse av personvernombudenes oppgaver basert på kravene i personopplysningsloven, og gir informasjon om prosjektets økonomiske rammer og varighet, og om tidspunkt for når prosjektet skal evalueres. Av prosjektinvitasjonen og prosjektavtalen sett under ett fremgår det at personvernombudet skal utføre følgende oppgaver:

- Informere og gi råd til behandlingsansvarlige
- Kontrollere overholdelse av personvernregelverket
- Samle inn informasjon for å identifisere behandlingsaktiviteter
- Analysere og sjekke at behandlingsaktivitetene er i tråd med regelverket
- Informere, gi råd og anbefalinger for å sikre regelverketterlevelse
- Foreslå ansvarsfordeling for oppgaver knyttet til ivaretakelse av personvernet i virksomheten
- Gjennomføre holdningsskapende arbeid i virksomheten og opplæring av medarbeidere
- Gi råd om vurdering av personvernkonsekvenser
- Samarbeide med Datatilsynet og fungere som kontaktpunkt
- Prioritere innsatsen dit hvor personvernrisikoen er høyest
- Bidra til å få oversikt over behandlingene
- Være kontaktpunkt for de registrerte

Styret i IKA MR og daglig leder gav det fagansvarlige personvernombudet innledningsvis noen overordnete råd om områder det var viktig å være oppmerksom på i en oppstartsfase av arbeidet, men utover det har hun i stor grad fått "frie tøyler" når det gjelder å forme prosjektet Personvernombud.

Prosjektet har ikke blitt styrt iht. etablert prosjektmetodikk, men derimot mer som en driftsorganisasjon. Personvernombudene har ikke en funksjonsbeskrivelse, men forholder seg til dokumentet *Roller og oppgåver* som de selv har utarbeidet, og som baserer seg på Datatilsynets beskrivelse av personvernombudets rolle. Prosjektet har i liten grad formaliserte rammer. Eksempelvis foreligger det ikke et klart mandat for prosjektet, det er ikke dokumentert hvilke saker / beslutninger som skal eskaleres til hhv. daglig leder og styret i IKA MR, og det er ikke etablert en handlingsplan for prosjektet. Det er heller ikke tydeliggjort i hvilke kanaler prosjektdeltakerne kan gi "ris og ros" til prosjektet.

Personvernombudene opplevde det innledningsvis i prosjektet som litt krevende å skulle definere sin egen rolle og prosjektets rammer, parallelt med at de skulle ivareta rollen som personvernombud for 27 virksomheter. Ingen av personvernombudene hadde tidligere erfaring fra prosjekt- eller linjeledelse, og hadde ikke forutsetninger for å vite hvilke formaliserte rammer som burde vært etablert for et slikt prosjekt. Personvernombudene brukte innledningsvis en del tid på å definere sin egen rolle, hva prosjektet skulle innebære, og på å forstå "stammespråket" blant prosjektdeltakerne. De har tatt utgangspunkt i prosjektavtalen og egen kompetanse om rollen som personvernombud, og har etter beste evne fulgt opp rollen som personvernombud for prosjektdeltakerne. Der de har sett behov for det, har de løftet problemstillinger til diskusjon med daglig leder i IKA MR. I tillegg har fagansvarlig personvernombud på forespørsel fra daglig leder gitt en skriftlig rapport til hvert styremøte i IKA MR.

2.1.2 IKA MRs samhandling med prosjektdeltakerne

Personvernombudene beskriver et åpent og godt samarbeid med prosjektdeltakerne. De inviteres inn i ulike møter og samarbeidsfora hos prosjektdeltakerne, og har fått tilbakemeldinger på at de er gode samarbeidspartnere i arbeidet med å etterleve det nye personvernregelverket.

I det første året av prosjektet har hovedfokus vært på å rådgi og støtte prosjektdeltakerne, og ombudene har drevet liten grad av kontrollerende virksomhet (jf. avsnitt 2.7.2). De har gjennomført et fysisk oppstartsmøte med hver enkelt prosjektdeltaker, og har bla. brukt mye tid på å vurdere kommunenes databehandlingsavtaler og veiledning i deres arbeid med å etablere protokoll over behandlinger, i tillegg til at de har gjennomført halvårlige fagdager der aktuelle personvernrelaterte tema har blitt gjennomgått og diskutert. Det at en del av prosjektdeltakerne er svært umodne når det gjelder etterlevelse av personvernregelverket, har gjort at de har trengt mye støtte i arbeidet. Et eksempel som blir trukket frem av det ene personvernombudet her, er at han i tillegg til å bidra i kvalitetssikring av en databehandleravtale måtte delta i forhandlingene med databehandler for at avtalen skulle kunne landes.

Fagdagene har blitt godt mottatt av prosjektdeltakerne, som også har fått anledning til å utveksle erfaringer med hverandre. Ombudene har i tillegg brukt litt tid på holdningsskapende arbeid, og har en plan om å gjennomføre større grad av kontroller i tiden fremover. De arbeider for å redusere terskelen for å melde avvik hos prosjektdeltakerne, og forteller at de kommuniserer et "føre var prinsipp". Det oppleves som krevende å endre gamle vaner, og prosjektdeltakerne beskrives i varierende grad som forbedringsorienterte. Ombudene opplever det også som krevende å få enkelte prosjektdeltakere til å prioritere arbeidet med personvern tilstrekkelig høyt.

Kontaktpersonene hos prosjektdeltakerne er typisk rådgivere og mellomledere. Personvernombudene forteller at det er vanskelig å sørge for at informasjon spres videre ut i prosjektdeltakernes virksomhet, både til ledelsen og i virksomheten for øvrig. Fagansvarlig personvernombud fortalte at det har hendt at hun har sendt brev til arkivet hos prosjektdeltakerne, for å sikre at brevet journalføres.

Fagansvarlig personvernombud forteller at det ikke ble utarbeidet en "standard informasjonspakke" som ble gitt til alle prosjektdeltakerne innledningsvis i prosjektet. Hun legger til grunn at det ville ha vært hensiktsmessig for å sikre at alle fikk den samme informasjonen i en tidlig fase, og at det bør utarbeides en slik for gjennomgang med eventuelle nye prosjektdeltakere. Generelt har personvernombudene vært opptatt av å klargjøre roller og ansvar, og fagansvarlig personvernombud forteller at hun har "åpnet nesten alle møter" med å opplyse om innholdet i ombudsrollen, at den er rådgivende, og plassere beslutningsansvaret hos prosjektdeltakerne. Ombudene opplever at det fremstår som relativt klart for prosjektdeltakerne hvilket ansvar de har, og at det er selv som må lage rutiner osv. Ombudene og enkelte prosjektdeltakere uttrykker imidlertid at de er usikker på om rolle- og ansvarsfordelingen fremstår som like klar for toppledelsen i virksomheten.

Det er stor variasjon i hvor mye de ulike prosjektdeltakerne har arbeidet for å etterleve regelverket, og det er derfor også stor variasjon når det gjelder hvor langt de har kommet. Det gjør at de har ulike behov, og ombudene har forsøkt å skreddersy rådgivningen de har gjort inn mot den enkelte prosjektdeltaker.

Personvernombudene har tatt i bruk delingsplattformen *Teams* for å kommunisere med prosjektdeltakerne, og har en målsetting om å i størst mulig grad gi informasjon til alle prosjektdeltakerne samtidig. Det er imidlertid ikke alle prosjektdeltakerne som vet at Teams benyttes som en kommunikasjonsplattform i prosjektet, og andre har ikke tatt det i bruk. Det skal være mulig for prosjektdeltakerne å gi tilbakemeldinger til prosjektet via Teams, men det var det ingen av prosjektdeltakerne som ble intervjuet som var klar over.

Våren 2019 ble det etablert en referansegruppe for prosjektet. IKA MR hadde valgt ut enkelte prosjektdeltakere som ble invitert inn i gruppen. Det er gjennomført et møte i referansegruppen. Personvernombudene fikk i det møtet mye positive tilbakemeldinger på det arbeidet som gjøres, og det fremkom også noen anbefalinger til justeringer av prosjektet. Dette gikk blant annet på å i større grad legge til rette for erfaringsdeling mellom prosjektdeltakerne, samt å benytte Teams mer aktivt for å publisere faglige vurderinger og generelle personvernbetraktninger.

Personvernombudene legger til grunn at de får fulgt opp prosjektdeltakerne "godt nok", men at det kan være behov for at de tar en mer proaktiv rolle. Ombudene vektlegger å følge opp henvendelser raskt, helst samme dag som de kommer inn. Ombudene erkjenner at det er en ujevn fordeling av fokus på prosjekt-deltakerne, der de bruker mer tid på dem som ofte tar kontakt og ber om råd. Fagansvarlig personvern-ombud legger til grunn at det er behov for å fokusere mer på de mindre kommunene fremover. Et av personvernombudene forteller at det er krevende å være ombud for et så stort antall virksomheter.

2.1.3 Læring av prosjektet – vår vurdering

Uavhengig av om personvernombudsrollen ble definert som et prosjekt eller som en del av IKA MRs driftsorganisasjon, burde rammene for personvernombudene i større grad vært tydeliggjort. Det burde blant annet vært etablert et mandat, tydeliggjort hvilke beslutninger som skal eskaleres til hvilket beslutningsnivå og rutiner for evaluering og læring.

I en tidlig fase av arbeidet burde det vært etablert en handlingsplan med viktige milepæler for personvernombudene, gjerne kombinert med et årshjul med faste aktiviteter som skal gjennomføres. En tydeliggjøring av forventninger og rammer er ekstra viktig i en situasjon der personvernombudene har svært begrenset erfaring fra arbeidslivet generelt, og fra tilsvarende roller spesielt.

IKA MR har lykkes med å rekruttere gode kandidater til å ivareta personvernombudsrollen. Personvernombudene leverer tjenester som prosjektdeltakerne jevnt over er godt fornøyd med. Begge ombudene oppleves som faglig dyktige og til å ha personlige egenskaper som gjør dem godt egnet til å ivareta en slik rolle. Prosjektet har således i stor grad klart å oppfylle prosjektdeltakernes forventninger, til tross for begrenset grad av styring og kontroll. Det er imidlertid likevel behov for å gjøre noen justeringer av personvernombudenes arbeid. Utdypning av denne problemstillingen fremgår av avsnitt 2.7.3, og forslag til hvordan dette kan gjøres fremgår av kapittel 3 – Anbefalinger.

2.2 Hvilke erfaringer har prosjektdeltakerne med ordningen?

Prosjektdeltakerne uttrykker jevnt over at de er godt fornøyd med jobben personvernombudene gjør, at de er gode samarbeidspartnere og støttespillere, og at dagens løsning der de ivaretar ombudsrollen for virksomheten er en bedre løsning enn det de ville fått til ved å ha et internt personvernombud. Representantene for prosjektdeltakerne som ble intervjuet uttrykte alle at de ønsket en forlengelse av samarbeidet etter 2020, samtidig som flere presiserte at det ikke var opp til dem å fatte den beslutningen.

Personvernombudets kompetanse

Samtlige av prosjektdeltakerne som ble intervjuet uttrykte at de opplevde at personvernombudet hadde tilstrekkelig kompetanse innen personvern. Flere ser styrken i at det er to ulike ombud som samarbeider og dermed får tilgang på ytterligere kompetanse i krevende saker. Flere pekte på at ombudene gjennom sitt arbeid stadig tilegnet seg ny relevant kompetanse om deres virksomhet.

Enkelte pekte på at det kunne ha vært en fordel dersom ombudene hadde hatt en litt mer ulik utdannelse / bakgrunn. Teknisk kompetanse og erfaring fra kommunal sektor ble trukket frem som områder der økt kompetanse kan være verdifullt. Enkelte fortalte at det har vært noen innledende utfordringer grunnet begrenset kompetanse om deres virksomhet, og om hvordan beslutningsprosesser foregår i kommunal sektor.

Personvernombudets mandat

Prosjektdeltakerne er kjent med personvernombudenes mandat gjennom dokumentene "Prosjektinvitasjon - felles personvernombud" og "Prosjektavtale". I begge disse dokumentene listes arbeidsoppgavene som personvernombudet skal ivareta opp, og innholdet er i tråd med lovkrav. Førstnevnte dokument henviser også til oversikt i Artikkel 39 og til veileder hos Datatilsynet, hvor personvernombudets oppgaver er hentet fra.

Samarbeidsplattformen Teams

Personvernombudene har tatt i bruk samarbeidsplattformen Teams for å kommunisere med prosjektdeltakerne og dele informasjon og dokumentasjon. Ikke alle prosjektdeltakerne kjenner til eller har tatt i bruk Teams, og ingen av dem var klar over at de kunne gi tilbakemeldinger på samarbeidet i denne kanalen.

De som brukte Teams, fortalte at det var en god plattform for å kommunisere og dele informasjon med personvernombudet. Enkelte etterspurte at det kunne brukes mer, både til erfaringsdeling og til deling av personvernrelatert informasjon.

Personvernombudets kapasitet

Slik ordningen er i dag, hvor ombudet i stor grad har fokus på den rådgivende delen av stillingen, opplever samtlige av prosjektdeltakerne som ble intervjuet at de får den hjelpen de trenger innen rimelig tid. Det er flere som trekker frem at ombudet deres er lett tilgjengelig og alltid klar for å håndtere innkommende henvendelser. Ordningen er fortsatt i en tidlig fase, og det er ikke alle oppgaver som følger av "personvernombudenes mandat" som har blitt fulgt opp i stor grad.

I forbindelse med at ombudet etter hvert i større grad skal ivareta kontrolloppgaver, er det flere prosjektdeltakere som uttrykker usikkerhet ifht. om ombudets kapasitet er tilstrekkelig. Når ombudet utfører alle avtalte oppgaver i et visst omfang, vil det resultere i økt arbeidsbelastning.

Informasjon om rollen til personvernombudet

Det ble gjennomført et introduksjonsmøte med kontaktpersonen hos hver prosjektdeltaker, der personvernombudet introduserte seg selv. Utover dette er det ikke gjennomført aktiviteter eller sendt ut skriv fra personvernombudet for å tydeliggjøre ombudets rolle. Ombudsrollen er imidlertid ofte tema i møter, og prosjektdeltakerne opplever at det er relativt tydelig hva som inngår i rollen. Enkelte legger imidlertid til grunn at det ikke nødvendigvis fremstår like tydelig for virksomhetens ledelse. Toppledelsen hos enkelte prosjektdeltakere trodde, i hvert fall tidligere, at personvernombudet hadde et større ansvar for deres etterlevelse av personopplysningsloven enn det som tilligger deres stilling.

Personvernombudets kontrollerende funksjon

Prosjektdeltakerne forteller at personvernombudet så langt primært har fungert som rådgiver, og i liten grad har utført kontroll av virksomhetens etterlevelse av regelverket. Ombudet har så vidt begynt å gjennomføre noen kontroller. Prosjektdeltakerne ble bedt om å fylle ut en egenevaluering høsten 2018, og enkelte har nylig blitt bedt om å oversende personvernerklæring og protokoll for at ombudet skal kontrollere innholdet i dokumentene. Flere prosjektdeltakere la til grunn at det var på tide at ombudet i større grad kontrollerte deres etterlevelse av regelverket.

Personvernombudet som rådgiver og sparringspartner

Noen av prosjektdeltakerne fortalte at de alltid inkluderer personvernombudet når de gjør personvernrelaterte vurderinger, mens andre fortalte at de bare inkluderer ombudet i vurderinger som oppleves som utfordrende.

Ingen av prosjektdeltakerne som ble intervjuet hadde fullført en personvernkonsekvensvurdering (DPIA). En prosjektdeltaker fortalte at de hadde påbegynt arbeidet, og at ombudet hadde blitt invitert til å delta i en workshop i den forbindelse. En annen fortalte at de hadde begynt å diskutere at det måtte gjøres, og at de da ville involvere personvernombudet i arbeidet, men at de ikke var sikker på om det ville skje i selve arbeidet, eller i etterkant for å kvalitetssikre arbeidet.

Personvernombudet som kontaktpunkt med Datatilsynet

Det fremgår av dokumentet *Prosjektinvitasjon – felles personvernombud* at personvernombudet skal samarbeide med Datatilsynet og fungere som kontaktpunkt mot dem. Gjennom intervjuer fremgår det at det er ulik kjennskap til dette. En av prosjektdeltakerne var tydelig på at det var personvernombudet som skulle følge opp kontakten med Datatilsynet. En annen prosjektdeltaker la til grunn at de selv hadde ansvaret for å følge opp denne kontakten.

Personvernombudets rolle ved etablering og oppdatering av protokoll over behandlinger

Det varierer hvor langt de ulike prosjektdeltakerne har kommet når det gjelder å etablere og oppdatere en oversikt over behandlinger av personopplysninger. Ombudet har hatt en rådgivende rolle hos flere av prosjektdeltakerne i arbeidet med å etablere en slik oversikt.

Fordeling av ansvar ved sikkerhetsavvik

Det fremgår ikke av *Prosjektinvitasjon – felles personvernombud* eller av prosjektavtalen at personvernombudet skal melde avvik. Dette er prosjektdeltakerne innforstått med, og samtlige av de som ble intervjuet mente virksomheten selv hadde ansvaret for å følge dette opp. Ombudet ble imidlertid beskrevet som en viktig diskusjonspartner og rådgiver i slike saker.

Personvernombudets rolle ved utarbeidelse av rammeverk og styrende dokumentasjon

Prosjektdeltakerne og personvernombudet virker å være samstemt når det gjelder ansvar og rollefordeling for rammeverk og styrende dokumentasjon. Prosjektdeltakerne forteller at personvernombudene har en rådgivende rolle ved utarbeidelse av rammeverk, og styrende dokumentasjon, rutiner og maler innen personvern. Flere fortalte at de hadde brukt ombudene aktivt som diskusjonspartnere og rådgivere i dette arbeidet, blant annet ved utforming av databehandleravtaler, og de opplevde at de fikk rask og god bistand fra ombudet.

Ombudene har samarbeidet om å utarbeide en mal for databehandleravtaler og en veiledning for gjennomføring av personvernkonsekvenser, som skal være tilgjengelig for alle prosjektdeltakerne i samarbeidet. Ikke alle prosjektdeltakerne var klar over at disse dokumentene eksisterer.

Personvernombudets synlighet i virksomhetene

Prosjektdeltakerne forteller at de har informert om ombudet i personvernerklæringen og på internett og intranett. Det er i liten grad gjort ytterligere tiltak for å synliggjøre personvernombudet hos prosjektdeltakerne, verken fra virksomhetens eller ombudets side.

2.3 Har personvernombudet en tilstrekkelig uavhengig stilling?

2.3.1 Krav i personopplysningsloven

Artikkel 38 i personvernforordningen adresserer personvernombudets stilling. Av punkt 3 fremgår følgende:

Den behandlingsansvarlige og databehandleren skal sikre at personvernombudet ikke mottar instrukser om utførelsen av nevnte oppgaver. Vedkommende skal ikke avsettes eller straffes av den behandlingsansvarlige eller databehandleren for å utføre sine oppgaver. Personvernombudet skal rapportere direkte til det høyeste ledelsesnivået hos den behandlingsansvarlige eller databehandleren.

Dokumentet *Guidelines on Data Protection Officers* utdyper i punkt 3.3 kravet til uavhengighet, og presiserer blant annet at (teksten er fritt oversatt fra engelsk):

(…) Personvernombud må ikke instrueres når det gjelder hvordan de skal håndtere en sak, for eksempel, hvilke resultater som skal oppnås, hvordan de skal etterforske en klage eller om de skal konsultere tilsynsmyndigheten. Videre må de ikke instrueres til at de skal uttrykke et bestemt syn på en personvernrelatert problemstilling, eksempelsvis en bestemt tolkning av regelverket.

Videre understreker veiledningen at personvernombudets autonomi ikke innebærer at det har beslutningsmyndighet utover det som følger av artikkel 39, og at det er den behandlingsansvarlige eller databehandleren som er ansvarlig for etterlevelse av regelverket og som må demonstrere compliance.

2.3.2 Dagens praksis

Det fagansvarlige personvernombudet forteller at ombudene starter de fleste møter med å informere om hva som inngår i rollen personvernombud, samt hvilket ansvar som påhviler den enkelte virksomhet. Både personvernombudene og prosjektdeltakerne som har blitt intervjuet legger til grunn at det er relativt tydelig avklart hvilken rolle og ansvar som påhvilker hhv. ombudet og den enkelte virksomhet, og begge parter er kjent med at personvernombudet skal ha en uavhengig rolle, og har anledning til å varsle Datatilsynet dersom de er mener at en prosjektdeltakers praksis i betydelig grad bryter med gjeldende lovkrav. Personvernombudene legger til grunn at de i en relativt tidlig fase med nye lovkrav har hovedfokus på å bistå prosjektdeltakerne slik at de kan få en bedre praksis.

Flere forteller at det ikke virker å være en like god forståelse av rolle- og ansvarsfordelingen mellom personvernombudet og virksomheten, hos enkelte av prosjektdeltakernes ledelse. Det fremgår ikke av prosjektavtalen eller av annen dokumentasjon vi har fått tilsendt, hvem personvernombudet formelt rapporterer til hos prosjektdeltakerne. I praksis har hver prosjektdeltaker oppnevnt en kontaktperson for ombudet, som typisk er en rådgiver eller mellomleder i virksomheten. Fagansvarlig personvernombud forteller at det kan være krevende å få innpass i ledermøter for å informere om ombudsrollen. At ledelsen har en travel agenda og kan ha utfordringer med å prioritere samhandling med personvernombudet bekreftes også av flere prosjektdeltakere.

Verken personvernombudene selv, daglig leder i IKA MR, eller prosjektdeltakerne som ble intervjuet uttrykker at personvernombudets uavhengighet har blitt utfordret. Personvernombudene gir tydelige råd og veiledning, og har ikke opplevd å bli presset til å uttrykke et annet standpunkt.

Det har forekommet situasjoner der prosjektdeltakere har valgt å innta et annet standspunkt enn personvernombudet. I slike tilfeller har det vært tydelig for begge parter at ombudet har en rådgivende rolle, og at det er den enkelte prosjektdeltaker som beslutter hva som skal gjøres. Personvernombudet har dokumentert sine vurderinger, men har ikke vurdert det slik at det har skjedd et så alvorlig personvernbrudd at det har vært nødvendig å varsle Datatilsynet.

2.3.3 Vurdering av gjeldende praksis

KPMG har ingen indikasjoner på at en eller flere prosjektdeltakere har forsøkt å instruere personvernombudet i sitt arbeid, og således har utfordret ombudets uavhengige stilling.

For at Personvernombudet skal ha en uavhengig stilling, er det et viktig kriterium at vedkommende skal rapportere til virksomhetens øverste leder. Vi har ikke sett dokumentasjon på at dette er praksis for deltakerne i prosjektet. Kravet til at ombudet skal rapportere til øverste leder innebærer også at ombudet i tilstrekkelig grad må få anledning til å kommunisere med øverste leder. Det er således viktig at den enkelte prosjektdeltaker sørger for at ombudet får "tilgang på" øverste leder når ombudet uttrykker at det er nødvendig, for at lovens krav skal kunne anses å være oppfylt.

Vår vurdering er at personvernombudene delvis oppfyller kravene i personopplysningsloven mht. å ha en tilstrekkelig uavhengig stilling. Ombudene forsøkes ikke påvirket av prosjektdeltakerne, men det er indikasjoner på at ombudet i praksis ikke rapporterer til virksomhetens øverste leder hos enkelte av prosjektdeltakerne.

2.4 Har personvernombudet tilstrekkelig kompetanse og forståelse for virksomheten?

2.4.1 Krav i personopplysningsloven

Artikkel 37 i personvernforordningen om utpeking av personvernombud adresserer personvernombudets kvalifikasjoner og ekspertise. Av punkt 5 fremgår følgende:

Personvernombudet skal utpekes på grunnlag av faglige kvalifikasjoner og særlig på grunnlag av dybdekunnskap om personvernlovgivning og praksis på området samt evne til å utføre oppgavene nevnt i artikkel 39.

Dokumentet *Guidelines on Data Protection Officers* utdyper i vedlegget *DPO Guidelines: What you need to know,* punkt 8, kravet til kompetanse som følger (teksten er fritt oversatt fra engelsk):

Det nødvendige kompetansenivået avhenger av databehandlingsaktivitetene som utføres, og det beskyttelsesnivået som er nødvendig for persondataene som behandles. Eksempelvis vil det være behov for høyere kompetanse i tilfeller der en behandlingsaktivitet er særlig kompleks, eller der store mengder data med et særlig beskyttelsesbehov behandles.

Relevante kvalifikasjoner og ekspertise inkluderer:

- *Ekspertise i nasjonal og Europeisk personvernlovgivning og praksis inkludert en dyptgående forståelse for Personvernforordningen (GDPR)*
- *Forståelse for behandlingsaktivitetene som utføres*
- *Forståelse for informasjonsteknologi og datasikkerhet*
- *Kunnskap om forretningsområdet og virksomheten*
- *Evne til å være en pådriver for en betryggende personvernkultur i virksomheten*

2.4.2 Dagens praksis

Begge personvernombudene er utdannet jurister med fordypning innen personvern, og en av dem har også noe fordypning innen datasikkerhet. Både daglig leder ved IKA MR og personvernombudene legger til grunn at de har stor frihet når det gjelder deltakelse på kurs, seminarer og i andre fora, for å bygge nødvendig kompetanse for å kunne utføre rollen som personvernombud på tilfredsstillende vis.

Alle prosjektdeltakerne som ble intervjuet fortalte at ombudene oppleves som kompetente til å fylle rollen sin, og flere legger til grunn at det trolig ikke ville vært mulig for et internt ombud å ha en like sterk kompetanse på området. Dette begrunnes både med at ombudene er "heltidsombud" med anledning til full konsentrasjon om fagfeltet og ombudsrollen, og med gevinster som følge av læring på tvers av de ulike prosjektdeltakerne, og ved at ombudene inngår i et fellesskap der de kan lære av hverandre.

Prosjektdeltakerne forteller at de får raske tilbakemeldinger på spørsmål de sender ombudene, at svarene de får er godt begrunnet, og at det legger til rette for et effektivt personvernarbeid internt i virksomheten. Ombudene på sin side forteller at det tidvis er store arbeidsmengder, men at de bestreber å svare på spørsmål fra prosjektdeltakerne raskt, aller helst samme dag som henvendelsen kom.

Enkelte forteller at det i en tidlig fase tidvis virket å være litt krevende for personvernombudene å forstå virksomheten og de behandlingsaktivitetene som ble utført, men at ombudene har opparbeidet seg verdifull erfaring gjennom arbeidet og nå har fått en tilfredsstillende forståelse for virksomheten.

Jevnt over uttrykker prosjektdeltakerne at de er svært tilfreds med ombudenes kompetanse. De forteller at ombudene er fremoverlente og "på selgeren", bidrar aktivt i fora de inviteres inn i, og at de er en pådriver for å utvikle en bedre personvernkultur i virksomheten. Prosjektdeltakerne beskriver ombud som tør å stå for sine standpunkt, og som de regner med vil være i stand til å argumentere overfor virksomhetens øverste ledelse om hvorfor det er nødvendig å ta grep for å etterleve lovkrav, dersom de opplever det som nødvendig.

2.4.3 Vurdering av gjeldende praksis

De to personvernombudene i IKA MR er ombud for totalt 27 virksomheter, hvorav 26 kommuner samt for Møre og Romsdal Fylkeskommune. Virksomhetene de er personvernombud for behandler personopplysninger om innbyggerne, derunder helseopplysninger, opplysninger om skoleelever m.v. Virksomhetene behandler således store mengder data med et særlig beskyttelsesbehov, og det er således iflg. personopplysningsloven behov for at ombudene innehar særlig høy kompetanse.

Begge ombudene har relevant utdannelse og fordypning, og jobber aktivt med å bygge ytterligere relevant kompetanse parallelt med arbeidet som personvernombud, blant annet gjennom ISO-sertifisering og kurs innen risikostyring, i tillegg til deltakelse i ulike personvernfora. Tett samhandling med prosjektdeltakere i forbindelse med ulike problemstillinger og avvik, og deltakelse i ledermøter og andre fora, har bidratt til økt forståelse for virksomhetene og de behandlingsaktiviteter de utfører.

Personvernombudene forteller selv at de opplever å ha relativt god forståelse for informasjonsteknologi og datasikkerhet, og dette underbygges av prosjektdeltakerne som sier ombudene har tilstrekkelig forståelse til å ivareta ombudsrollen på en god måte. Et av ombudene har også noe fordypning innen datasikkerhet, og kompetansen videreutvikles og holdes relevant gjennom deltakelse i ulike fora.

Begge personvernombudene fremstår som kompetente og "uredde". De har valgt en tilnærming til prosjektdeltakerne der de først og fremst ønsker å bidra som rådgivere til prosjektdeltakerne i 2018 og 2019, og har valgt å nedtone kontrolldimensjonen av arbeidet (jf. avsnitt 2.7.2). Denne prioriteringen er gjort fordi de vurderte det som mest hensiktsmessig gitt at prosjektdeltakerne jevnt over var relativt umodne i sitt arbeid for å etterleve personvernkrav. Det at ombudene i begrenset grad har utført kontroller av virksomhetene, og heller ikke har gjennomført en systematisk risikovurdering av risikoen for personvernbrudd i den enkelte virksomhet, gjør at det fremstår som uklart hvorvidt personvernombudene har tilstrekkelig forståelse for aktuelle personvernrelaterte problemstillinger i virksomheten.

Vår vurdering er at personvernombudene virker å oppfylle kravene til kvalifikasjoner og ekspertise som følger av personopplysningsloven.

2.5 Involveres personvernombudet i alle spørsmål som gjelder vern av personopplysninger?

2.5.1 Krav i personopplysningsloven

Artikkel 38 i personvernforordningen om Personvernombudets stilling adresserer personvernombudets posisjon i virksomheten. Av punkt 1 fremgår følgende:

Den behandlingsansvarlige og databehandleren skal sikre at personvernombudet på riktig måte og i rett tid involveres i alle spørsmål som gjelder vern av personopplysninger.

Guidelines on Data Protection Officers utdyper videre i punkt 3.1 kravet i POL artikkel 38 (1). Utdrag av veiledningen følger under (teksten er fritt oversatt fra engelsk):

(…) Når det gjelder personvernkonsekvensvurderinger, krever Personvernforordningen eksplisitt at personvernombudet involveres i en tidlig fase, og spesifiserer at ombudets råd skal innhentes ved slike vurderinger. (…) det er viktig at personvernombudet blir ansett som en diskusjonspartner internt i virksomheten, og at han eller hun er en del av de relevante arbeidsgrupper som jobber med databehandlingsaktiviteter internt.

Som en konsekvens av dette, må virksomheten eksempelvis sikre at:

- *Personvernombudet inviteres til å delta i jevnlige møter med toppledelsen og ledelsen på mellomnivå.*
- *Hans eller hennes tilstedeværelse anbefales når beslutninger av betydning for personvernet fattes. All relevant informasjon må raskt gjøres tilgjengelig for personvernombudet for å gjøre ham eller henne i stand til å gi relevante råd.*
- *Meningen til personvernombudet må alltid vektlegges tilstrekkelig. I tilfeller med uenighet, anbefaler WP29 (arbeidsgruppen), som en god praksis, at grunnlaget for å avvike fra personvernombudets anbefaling dokumenteres.*
- *Personvernombudet må omgående konsulteres med en gang et personvernavvik eller en annen personvernrelatert hendelse har inntruffet.*

2.5.2 Dagens praksis

Alle prosjektdeltakerne som ble intervjuet la til grunn at personvernombudene var gode diskusjonspartnere, som de brukte aktivt ved ulike personvernrelaterte problemstillinger. Personvernombudene er på sin side opptatt av å være tilgjengelig som rådgivere, og bestreber å delta på alle møter de blir invitert til, og svare raskt og med god kvalitet på alle forespørsler de mottar fra prosjektdeltakerne.

Ingen av prosjektdeltakerne vi var i kontakt med hadde fullført en personvernkonsekvensvurdering. En prosjektdeltaker fortalte at de hadde startet et slikt arbeid, og at personvernombudet deltok i dette arbeidet, blant annet gjennom deltakelse i en workshop. En annen prosjektdeltaker fortalte at de regnte med å begynne dette arbeidet snart, og at de da ville sørge for å involvere personvernombudet i de vurderingene

som skulle gjøres. Flere prosjektdeltakere fortalte at de jevnlig inviterte personvernombudet inn i ulike fora der personvernrelaterte problemstillinger diskuteres.

I følge personvernombudene er det hos en del prosjektdeltakere krevende å få tilstrekkelig innpass hos toppledelsen. Dette skal særlig være tydelig hos prosjektdeltakere som er i en fusjonsprosess med andre kommuner, og som konsentrerer mye av ressursbruken sin rundt den planlagte fusjonen. Flere prosjektdeltakere bekrefter at slike pågående prosesser tar mye tid, og at det bidrar til at det er krevende å prioritere personvernområdet tilstrekkelig, både for ledelsen og for virksomheten for øvrig.

Både personvernombudene og prosjektdeltakerne forteller at ombudet involveres ved viktige personvernrelaterte vurderinger, derunder i situasjoner der det er oppdaget et personvernrelatert avvik. Prosjektdeltakerne følger i de fleste tilfeller ombudets råd. Det har forekommet situasjoner med uenighet mellom partene. I slike tilfeller forteller ombudet at det har vært påpasselig med å dokumentere sitt standpunkt, og begrunnelsen for dette.

2.5.3 Vurdering av gjeldende praksis

Personvernombudene inviteres til dialog om personvernrelaterte problemstillinger, og tas med på råd når det oppdages avvik av et visst omfang.

Hos flere av prosjektdeltakerne er det utfordrende for ombudet å få tilstrekkelig innpass i toppledelsen. Dette kan bidra til redusert forståelse for ansvars- og rollefordelingen mellom virksomheten og personvernombudet, til at viktige problemstillinger ikke i tilstrekkelig grad drøftes mellom personvernombudet og toppledelsen, og til at det kan bli krevende for ombudet å gå i dialog med øverste leder i situasjoner med uenighet mellom ombudet og medarbeidere lenger nede i virksomheten.

Vår vurdering er at prosjektdeltakerne i enda større grad bør legge til rette for at personvernombudet skal få en hensiktsmessig posisjon i virksomheten, blant annet ved å sørge for at ombudet får nødvendig tilgang til toppledelsen, for å sikre etterlevelse av lovkrav.

2.6 Har personvernombudet nødvendige ressurser til å ivareta ombudsrollen?

2.6.1 Krav i personopplysningsloven

Artikkel 37 i personvernforordningen om utpeking av et personvernombud adresserer bla. at offentlige myndigheter kan ha felles ombud. Av punkt 3 fremgår følgende:

Dersom den behandlingsansvarlige eller databehandleren er en offentlig myndighet eller et offentlig organ, kan det utpekes ett personvernombud for flere av nevnte myndigheter eller organer, i det det tas hensyn til deres organisasjonsstruktur og størrelse.

Doumentet *Guidelines on Data Protection Officers* utdyper i punkt 2.3 POL artikkel 37 (3). Utdrag av veiledningen følger under (teksten er fritt oversatt fra engelsk):

(…) De samme betraktningene gjelder mht. ressurser og kommunikasjon. Gitt at personvernombudet har ansvar for en rekke oppgaver, må den behandlingsansvarlige og databehandleren sikre at personvernombudet, om nødvendig støttet av et team, kan utføre oppgavene effektivt til tross for at vedkommende har ansvar for flere offentlige virksomheter.

Artikkel 38 i personvernforordningen om Personvernombudets stilling adresserer nødvendige ressurser til å ivareta ombudsrollen. Av punkt 2 følger det at:

Den behandlingsansvarlige og databehandleren skal støtte personvernombudet i forbindelse med utførelsen av oppgavene nevnt i artikkel 39 ved å stille til rådighet de ressurser som er nødvendig for å utføre nevnte oppgaver, samt gi tilgang til personopplysninger og behandlingsaktiviteter og gjøre det mulig for vedkommende å opprettholde sin dybdekunnskap.

Dokumentet *Guidelines on Data Protection Officers* utdyper i punkt 3.2 kravet i POL artikkel 38 (2). utdrag av veiledningen følger under (teksten er fritt oversatt fra engelsk):

Følgende elementer må særlig vurderes:

- *At toppledelsen aktivt støtter funksjonen som personvernombud (…)*
- *Tilstrekkelig tid for personvernombudet til å utføre pliktene sine (…). Å ha tilstrekkelig tid tilgjengelig for personvernombudets oppgaver er en grunnleggende forutsetning. (…). Det er også en god praksis å beslutte hvor mye tid som er nødvendig for å ivareta funksjonen, hvordan personvernombudets oppgaver skal prioriteres, og at personvernombudet (eller virksomheten) utarbeider en handlingsplan. (...)*
- *Offisiell kommunikasjon om personvernombudet til alle virksomhetens ansatte for å sikre at det er kjent at det er et personvernombud og hva som er dets oppgaver innad i virksomheten.*
- *Nødvendig tilgang til andre tjenester (…), slik at personvernombudet kan motta nødvendig støtte og informasjon.*
- *Kontinuerlig kompetanseutvikling. Personvernombud må få muligheten til å holde seg oppdatert når det gjelder utviklingen innenfor personvernområdet. (…)*

Generelt er det slik at jo mer komplekse og / eller sensitive behandlingsaktiviteter, jo mer ressurser må stilles til disposisjon for personvernombudet. Personvernfunksjonen må ha tilstrekkelig og effektive ressurser sett opp mot behandlingsaktivitetene som utføres.

2.6.2 Dagens praksis

De to personvernombudene er ombud for henholdsvis 13 og 14 virksomheter, hvilket gjør at de i snitt har om lag 7% av en full stilling til oppfølging av ombudsrollen hos den enkelte prosjektdeltaker. Personvernombudene forteller at det er travelt, men at de stort sett rekker over det de må gjøre, og at de opplever at tiden de har tilgjengelig er tilstrekkelig til at deres oppfølging av den enkelte prosjektdeltaker er forsvarlig. Alle prosjektdeltakerne som har blitt intervjuet forteller at de får god oppfølging av ombudet når de ber om råd / har behov for det. Flere stiller spørsmål ved om ombudet vil ha tilstrekkelig tid til ombudsrollen dersom det oppstår en situasjon med mange henvendelser fra de registrerte, og / eller når de i større grad utfører kontroll av virksomheten. Flere kommuner skal imidlertid slå seg sammen 1. januar 2020, og antall prosjektdeltakere vil da reduseres fra 27 til 19. Dette vil bidra til at personvernombudet får mer tid tilgjengelig per prosjektdeltaker.

Prosjektdeltakerne som ble intervjuet fortalte at det primært var informert om personvernombudet på virksomhetens internett og intranett, for å informere henholdsvis de registrerte og de ansatte. I følge personvernombudene varierer det mellom prosjektdeltakerne hvorvidt de primært oppgir kontaktinformasjon til personvernombudet, eller om de også informerer om personvernombudets oppgaver. Personvernombudene har i liten grad blitt invitert inn i ledergrupper eller i ulike virksomhetsområder for å presentere seg selv og ombudsrollen. En prosjektdeltaker fortalte at det var informert om personvernombudet og dets rolle på epost, og da som en del av et nano-kurs innen personvern.

Personvernombudene har i følge dem selv og daglig leder i IKA MR, stor frihet til selv å velge hvilke kurs og konferanser de ønsker å delta på for å bygge og vedlikeholde nødvendig kompetanse for å ivareta ombudsrollen. Begge har deltatt på ulike kurs og konferanser ved siden av ombudsrollen, og det personvernombudet som har det faglige ansvaret for prosjektet, deltar blant annet i et nettverk for personvernombud i norske fylkskommuner.

2.6.3 Vurdering av gjeldende praksis

Personvernombudene er ombud for henholdsvis 13 og 14 virksomheter, hvilket i snitt gjør at de har om lag 7% av en full stilling til oppfølging av ombudsrollen hos den enkelte prosjektdeltaker, eller i overkant av 2.5 timer per uke. Gitt at noe tid går med til administrasjon, reisevirksomhet og ulike kompetansehevende tiltak, reduseres tilgjengelig tid for å ivareta ombudsrollen tilsvarende. Frem til nå har personvernombudene primært hatt fokus på sin rådgivende rolle, og det har vært begrenset med henvendelser fra de registrerte. Personvernombudene har uttrykt at det i tiden fremover blir viktig å i større grad kontrollere virksomhetene de er ombud for (jf. avsnitt 2.7.2). Et sannsynlig scenario er at det før eller siden vil oppstå en situasjon med et stort antall henvendelser fra registrerte, gjerne parallelt i flere kommuner, eksempelvis som følge av kritiske personvernrelaterte medieoppslag. I en slik situasjon vurderes det som sannsynlig at personvernombudene vil få utfordringer med å ivareta alle lovpålagte oppgaver på en betryggende måte. Den planlagte reduksjonen i antall prosjektdeltakere fra 27 til 19 ved årsskiftet, vil på den annen side bidra til å frigi kapasitet hos personvernombudet.

Prosjektdeltakerne har gjort tilgjengelig informasjon om personvernombudet for de registrerte og for virksomhetens ansatte. I og med at de ansatte selv aktivt må oppsøke den aktuelle informasjonen, er det sannsynlig at det er relativt lav kjennskap til hvem som er personvernombud og hva som inngår i

ombudsrollen i deler av virksomhetene. Blant enkelte av prosjektdeltakerne vil kjennskapen til hva som inngår i ombudsrollen være lav fordi det ikke er gjort tilgjengelig informasjon om hva den omfatter.

Personvernombudene har god anledning til å bygge kompetanse, og benytter seg også av dette slik at de sørger for å ha oppdatert og relevant kompetanse. Høyt arbeidspress gir en risiko for at ombudene kan komme til å nedprioritere påfyll av relevant kompetanse i fremtiden.

Vi vurderer det som sannsynlig at personvernombudet pt. ikke har tilstrekkelig tid til å gjennomføre alle sine forpliktelser iht. regelverket på betryggende vis.

2.7 Ivaretar personvernombudene oppgavene på en tilfredsstillende måte?

2.7.1 Krav i personopplysningsloven

Artikkel 39 i personvernforordningen stiller følgende krav til oppgaver personvernombudet skal utføre:

1. Personvernombudet skal minst ha følgende oppgaver:

a) Informere og gir råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har i henhold til denne forordning (…).

b) Kontrollere overholdelsen av denne forordning (…) og den behandlingsansvarliges eller databehandleresn personvernretningslinjer, herunder fordeling av ansvar, holdningsskapende tiltak og opplæring av personellet som er involvert i behandlingsaktivitetene, og tilhørende revisjoner

c) På anmodning gi råd om vurderingen av personvernkonsekvenser og kontrollere gjennomføringen av den i henhold til artikkel 35

d) Samarbeide med tilsynsmyndigheten

e) Fungere som kontaktpunkt for tilsynsmyndigheten ved spørsmål om behandlingen, herunder forhåndsdrøftingene nevnt i artikkel 36, og ved behov rådføre seg med tilsynsmyndigheten om eventuelle andre spørsmål.

2. Personvernombudet skal ved utførelsen av sine oppgaver ta behørig hensyn til risikoene forbundet med behandlingsaktivitetene, idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i.

Dokumentet *Guidelines on Data Protection Officers* utdyper i punkt 4 hvilke oppgaver personvernombudet skal og kan utføre, og presiserer blant annet at (teksten er fritt oversatt fra engelsk):

(…) Som en del av ansvaret for å kontrollere etterlevelse, kan personvernombud særlig:
- *Samle inn informasjon for å identifisere behandlingsaktiviteter*
- *Analysere og sjekke hvorvidt behandlingsaktiviteter utføres i henhold til lovkrav*
- *Informere, rådgi og utstede anbefalinger til behandlingsansvarlig eller databehandler*

Kravet til å kontrollere etterlevelse innebærer ikke at personvernombudet personlig er ansvarlig ved tilfeller med brudd på regelverket. Personvernforordningen presiserer at det er den behandlingsansvarlige og ikke personvernombudet som har ansvar for å implementere passende tekniske og organisatoriske tiltak for å sikre og være i stand til å demonstrere at behandling utføres i henhold til forordningen. (…).

Videre presiserer veiledningen at det er den behandlingsansvarlige og ikke personvernombudet som skal gjennomføre personvernkonsekvensvurderinger, men at vedkommende skal søke råd hos ombudet.

Punkt 4.4 i veiledningen adresserer kravet til at personvernombudet må ha en risikobasert tilnærming til utførelsen av ombudsrollen, og presiserer blant annet at (teksten er fritt oversatt fra engelsk):

(…) I hovedsak stilles det krav til at personvernombudet prioriterer oppgaver og fokuserer innsatsen sin på områder som representerer en forhøyet personvernrisiko. (…) En slik selektiv og pragmatisk tilnærming

skal hjelpe personvernombudet til å rådgi den behandlingsansvarlige mht. hvilken metode som bør benyttes når det gjøres personvernkonsekvensvurderinger, hvilke personvernrelaterte områder som bør revideres, hvilken opplæring medarbeidere og ledere med ansvar for databehandlingsaktiviteter bør få, og hvilke behandlingsaktiviteter det er behov for å ha et høyere fokus på.

2.7.2 Dagens praksis

IKA MR har ivaretatt rollen som personvernombud på vegne av prosjektdeltakerne siden 25. mai 2018. I denne perioden har ombudenes hovedfokus vært på å rådgi og støtte prosjektdeltakerne i sitt arbeid for å etterleve regelverket. Ombudene har arrangert fagdager for å bidra til kompetanseheving på sentrale områder, de har deltatt på ulike arenaer for å rådgi behandlingsansvarlige og databehandlere, de har informerer ledelsen om hva som inngår i ombudsrollen, rådgitt virksomhetene ved personvernrelaterte avvik, bidratt i personvernkonsekvensvurderinger osv. Både daglig leder for IKA MR og personvernombudene har vurdert det slik at det var nødvendig å primært opptre som en støttespiller i en tidlig fase, for slik å muliggjøre etterlevelse av regelverket for prosjektdeltakerne. Ombudene har som følge av dette i liten grad hatt fokus på å utføre kontroller for å avdekke eventuelle personvernrelaterte avvik.

Personvernombudene har utarbeidet et *Forslag til en DPIA-prosedyre*, og gjort denne tilgjengelig for prosjektdeltakerne. En prosjektdeltaker har startet arbeidet med å gjøre en personvernkonsekvensvurdering, og involverer personvernombudet i dette arbeidet. I følge det fagansvarlige personvernombudet hadde ingen av prosjektdeltakerne fullført en personvernkonsekvensvurdering per juni 2019.

Personvernombudene samarbeider med Datatilsynet på vegne av prosjektdeltakerne, og fungerer som kontaktpunkt inn mot tilsynet. Personvernombudet har og i enkelte tilfeller meldt avvik til tilsynet på vegne av den enkelte prosjektdeltaker. Både personvernombudet og prosjektdeltakerne er av den oppfatning at den enkelte virksomhet som hovedregel selv bør melde personvernrelaterte avvik til Datatilsynet.

I november 2018 sendte personvernombudene ut et skjema der prosjektdeltakerne ble bedt om å fylle ut en del informasjon for å gjøre en egenevaluering mht. etterlevelse av personvernregelverket. En av prosjektdeltakerne har, til tross for gjentatte purringer, ikke returnert det utfylte skjemaet til personvernombudet. Ombudene har også startet et arbeid med å gjennomgå og kontrollere prosjektdeltakernes protokoller og personvernerklæringer, og har utarbeidet en *revisjonsprosedyre* for dette arbeidet. Arbeidet er planlagt sluttført innen utgangen av 2019.

Personvernombudene legger til grunn at arbeidet de gjør skal være risikobasert, at de viktigste risikoene bør prioriteres først, og de har blant annet tatt opp temaer på de to fagdagene de har arrangert basert på hvilke områder de opplever at prosjektdeltakerne har størst behov for informasjon om. Når det gjelder gjennomføring av kontroller, har ombudene valgt å gjennomføre samme kontroller inn mot alle prosjektdeltakerne. Det ene personvernombudet fortalte at de valgte å kontrollere områder i 2019 som de visste Datatilsynet hadde fokus på. Verken personvernombudet eller prosjektdeltakere virker å ha gjort en helhetlig vurdering av hvilke utfordringer og risikoer den enkelte prosjektdeltaker har for oppfyllelse av kravene i personopplysningsloven.

2.7.3 Vurdering av gjeldende praksis

Personvernombudene bruker mye ressurser på å rådgi prosjektdeltakerne generelt og i forhold til forespørsel ved utarbeidelse av DPIA i henhold til lovens krav. Ombudene samarbeider med Datatilsynet, og fungerer også som kontaktpunkt mellom prosjektdeltakerne og tilsynet.

Vår vurdering er at personvernombudene ikke i tilstrekkelig grad har vurdert hvilke utfordringer og risikoer prosjektdeltakerne har for oppfyllelse av kravene i personopplysningsloven. Det gjør det krevende for ombudene å prioritere oppgaver og fokusere innsatsen sin på områder som representerer en forhøyet personvernrisiko.

Personvernombudene har så vidt startet arbeidet med å kontrollere virksomhetenes etterlevelse av kravene i POL. Dette begrunnes med at prosjektdeltakerne jevnt over var relativt umodne innen personvern, og at det derfor var behov for å bistå dem for å etablere nødvendig rammeverk, dokumentasjon og rutiner, før det kunne kontrolleres. En av prosjektdeltakerne som ble intervjuet uttrykte at de var helt i oppstarten av arbeidet med å etterleve nye personvernkrav, mens de øvrige intervjuobjektene beskrev en situasjon der de var kommet lenger i arbeidet men der det fortsatt gjenstår en god del. Dette indikerer at det er et tydelig behov for at personvernombudene følger opp med kontroller, og basert på det rådgir virksomhetene om

hvordan de bør prioritere ressursene på området. Det er for øvrig bekymringsfullt at en av prosjektdeltakerne valgte å ikke returnere en utfylt "egenevaluering" av status for deres arbeid på personvernområdet høsten 2018, til tross for gjentatte påminnelser. Den nye personopplysningsloven trådte i kraft for over et år siden, og allerede ved ikrafttredelse var det et krav at virksomheter skulle etterleve alle kravene i loven. Ombudene er således på overtid når det gjelder å komme skikkelig i gang med kontroll av i hvilken grad prosjektdeltakerne etterlever regelverket, basert på en systematisk og helhetlig risikovurdering.

Det er vår vurdering at personvernombudene ikke fullt ut etterlever kravene i personopplysningsloven om å ivareta alle lovpålagte oppgaver på en betryggende måte. Dette gjelder kravet om en risikobasert tilnærming, og til å kontrollere at virksomhetene etterlever kravene i personopplysningsloven.

2.8 Hvordan håndteres slike tjenester av andre?

Dersom en behandlingsansvarlig eller databehandler plikter å ha personvernombud, kan rollen gis til en medarbeider eller til en person utenfor organisasjonen. Eksempelvis er det mange leverandører (typisk private, men også interkommunale samarbeidsformer o.l.) som tilbyr personvernombud som tjeneste. Når det gjelder behandlingsansvarlige eller databehandlere som er en offentlig myndighet eller et offentlig organ, kan det utpekes ett personvernombud for flere av nevnte myndigheter eller organer, idet det tas hensyn til deres organisasjonsstruktur og størrelse (såkalt felles personvernombud).

Dersom ombudet er internt må vedkommende være en fysisk person. Benyttes en ekstern leverandør, må det på tilsvarende vis tilbys en fysisk kontaktperson for virksomheten som leverandøren av tjenesten ivaretar ombudsrollen for. Ifølge Datatilsynet kan en fordel med å ha ombud internt i virksomheten være at vedkommende ofte kjenner virksomheten bedre, og dermed lettere kan fange opp problemstillinger som oppstår underveis. Eksterne ombud kan derimot ha den fordel at han eller hun har bred erfaring og kunnskap som kan være nyttig for virksomheter som opplever at det er utfordrende å tilegne seg den nødvendige kompetansen internt.

Ulike virksomheter har valgt ulike måter å organisere rollen som personvernombud på. Noen offentlige virksomheter har valgt å ha et internt personvernombud, andre har outsourcet det slik tilfellet er for prosjektdeltakerne i prosjektet Personvernombud, enten ved at de deler ombud med andre offentlige virksomheter, eller ved at de kjøper tjenesten fra en profesjonell tilbyder av rollen. Datatilsynet har publisert en oversikt over registrerte personvernombud. Utover det finnes det ikke en lett tilgjengelig oversikt over antall virksomheter det enkelte personvernombud er ombud for, eller over hvordan ulike virksomheter har organisert rollen.

Vi kan trekke frem noen eksempler på hvordan andre virksomheter har organisert personvernombudsrollen. Store kommuner som Oslo, Bergen, Trondheim og Stavanger kommune har internt personvernombud. Personvernombudet i Bergen kommune er i tillegg ombud for 8 andre kommuner. Tilsvarende er IKT-Nordhordland personvernombud for en håndfull kommuner i Hordaland. Haugesund kommune har et internt personvernombud som i tillegg er utleid som ombud til Karmøy kommune i en 15% stilling. Et kraftselskap på Veslandet har et internt personvernombud i en 50% stilling. Vi kjenner ikke til konkrete eksempler på personvernombud som er ombud for et like stort antall virksomheter som det som er tilfellet for IKA MR.

Uansett hvordan funksjonen organiseres, må kravene knyttet til personvernombudsrollen overholdes. Datatilsynet legger til grunn at hver virksomhet må kartlegge sine behov sett opp mot kravene og om disse blir ivaretatt i det valget som tas. Det betyr blant annet at organisasjonens størrelse, dets modenhet, behovet for bistand, tidsaspekt, hvor store regelverksendringene er, det aktuelle personvernombudets faglige kvalifikasjoner og tilgjengelighet har betydning for vurde. ringen som må gjøres. Datatilsynet har ikke gitt noen detaljert veiledning, eller eksemplifisert, hva de anser som en god / forsvarlig praksis på området.

3. Anbefalinger

3.1 Anbefalte justeringer av prosjektet Personvernombud

Prosjektet Personvernombud har pågått i overkant av et år. Det er vår vurdering at personvernombudene i IKA MR gjør et viktig arbeid for å bidra til å løfte prosjektdeltakerne på personvernområdet.

Ordningen legger til rette for et tett samarbeid mellom to personvernombud om å levere slike tjenester. Dette er gunstig både fordi det reduserer sårbarheten ved fravær og ved skifte av personvernombud, og fordi det lar personvernombudene være en del av et lite miljø, i motsetning til i mange andre virksomheter der det er et personvernombud som er alene om ombudsrollen, og som gjerne ivaretar rollen kombinert med andre oppgaver.

Selv om det gjøres mye godt arbeidet i prosjektet, har vi foreslått noen justeringer for å legge til rette for økt etterlevelse av regelverket og et enda mer effektivt arbeid. Disse følger under:

I. Tydeliggjøring av prosjektets mandat

Det er behov for å tydeliggjøre et mandat for personvernombudene. Dette bør gjøres både for å sikre at personvernombudene har en helhetlig og enhetlig tilnærming til arbeidet i tråd med lovkrav, for å bidra til å skape trygge rammer for arbeidet de skal gjøre, samt for å tydeliggjøre krav og forventninger overfor prosjektdeltakerne.

Mandatet bør, iht. god praksis for prosjektstyring, bla. inneholde informasjon om følgende:

- Hvilke oppgaver personvernombudet har, derunder en tydeliggjøring av tilgrensende oppgaver ombudet ikke skal ivareta
- Hvilke oppgaver og ansvar som tilligger den enkelte prosjektdeltaker
- Prosjektets økonomiske rammer
- Prosjektets varighet
- Handlingsplan med oversikt over viktige milepæler, kan med fordel kombineres med et årshjul over faste oppgaver for personvernombudet
- Tydeliggjøring av roller, inkl. at personvernombudet rapporterer til øverste leder hos den enkelte prosjektdeltaker
- Oversikt over hvilke problemstillinger som skal eskaleres til hvilket nivå hos hhv. beslutningstaker og i IKA MR
- Krav til evalueringer underveis, samt til sluttevaluering (dersom det besluttes at prosjektet skal etableres som en del av IKA MRs driftsorganisasjon bortfaller sistnevnte)

Prosjektets rammer må kommuniseres til både kontaktperson og beslutningstaker hos den enkelte prosjektdeltaker, hvorav sistnevnte, ideelt sett, bør godkjenne mandatet for å kunne delta i prosjektet.

II. Tydeliggjøring av viktige strukturer i prosjektet

Det er behov for å tydeliggjøre viktige strukturer og samhandlingsarenaer i prosjektet, for å legge til rette for et forutsigbart og effektivt samarbeid mellom personvernombudet og den enkelte prosjektdeltaker, derunder:

- Aktuelle samarbeidsfora i prosjektet (eksempelvis fagdager)
- Hvilke samhandlingsplattformer som skal benyttes (eksempelvis Teams)
- Tydeliggjøring av kanaler for tilbakemeldinger fra prosjektdeltakere
- Transparens rundt eventuelle referansegrupper / styringsgrupper, og mulighet for alle til å melde sin interesse for å delta
- Tydeliggjøre hvilke oppgaver som tilligger hhv. personvernombudet og den enkelte prosjektdeltaker

    - IKA MR kan vurdere å etablere en tjenestekatalog med oversikt over hvilke oppgaver som tilligger rollen personvernombud inn mot alle prosjektdeltakerne, samt evt. "tilleggsoppgaver" som den enkelte prosjektdeltaker kan bestille fra personvernombudet mot en tilleggskostnad, eksempelvis interne opplæringsseminar innen personvern, fasilitering av personvernkonsekvensvurderinger osv.
- Tydeliggjøre forventninger til prosjektdeltakerne (inkl. at personvernombudet skal rapportere til øverste leder, og ha tilgang til kommunikasjon med denne ved behov osv.).

III. Risikovurdering og utførelse av kontroller

Det er behov for at personvernombudet i større grad kontrollerer den enkelte prosjektdeltakers etterlevelse av personopplysningsloven, samt eventuelle interne krav. Kontroller må være basert på en risikovurdering for å legge til rette for en hensiktsmessig prioritering og effektiv ressursbruk, og for å være iht. lovkrav.

Personvernombudet bør gjøre en helhetlig vurdering av hvilke utfordringer og risikoer prosjektdeltakerne har for oppfyllelse av kravene i personopplysningsloven. Ombudet bør se hen til eventuelle vurderinger av personvernrisiko som ledelsen hos den enkelte prosjektdeltaker har gjort, men bruke sitt eget skjønn i vurderingen av i hvilken grad det kan støtte seg på slike vurderinger. Dersom personvernombudet opplever at det ikke har tilstrekkelig informasjon til å vurdere utfordringer og risikoer hos den enkelte prosjektdeltaker, kan det være hensiktsmessig å gjøre en overordnet rammeverksrevisjon for å vurdere virksomhetens internkontroll, og basert på den identifisere hvilke områder det er knyttet særlig høy risiko til etterlevelsen av.

Ombudet bør deretter etablere en risikobasert handlingsplan over hvilke kontroller som skal utføres når hos den enkelte prosjektdeltaker. Ulik modenhet og fokus hos prosjektdeltakerne gjør at det vil være behov for ulike kontroller hos de ulike prosjektdeltakerne.

Risikovurderingen bør være et levende dokument som kontinuerlig oppdateres basert ny informasjon som blir tilgjengelig underveis i arbeidet. Eksempelvis vil egenevalueringer, personvernkonsekvensvurderinger, resultat av kontroller og tilsyn m.v. gi viktig informasjon i arbeidet med risikovurderinger.

IV. Vurdering av ressursbehov

Det bør gjøres en vurdering av om prosjektet har tilstrekkelig ressurser til at personvernombudene ivaretar alle sine oppgaver iht. lovkrav og prosjektavtalen på en betryggende måte. Personvernombudene har per i dag en hektisk arbeidshverdag som følge av at de er ombud for et stort antall virksomheter, hvorav mange har behov for mye støtte fordi de har begrenset med egne ressurser på personvernområdet samtidig som de er relativt umodne i arbeidet. Det forventes at en del av prosjektdeltakerne vil ha behov for betydelig grad av rådgivning i flere år fremover.

Ved økt grad av kontroll av virksomhetenes etterlevelse må det vurderes om det er nødvendig og hensiktsmessig å utvide prosjektets kapasitet. Vurderingen av ressursbehov må imidlertid ta høyde for at antall prosjektdeltakere reduseres fra 27 til 19 fra og med 1. januar 2020.

4. Vedlegg

3.1 Personopplysningsloven

Under følger utvalgte deler av Personopplysningsloven som er særlig relevant for rollen Personvernombud.

Kapittel 5. Personvernombud

§ 18.Personvernombudets taushetsplikt

Personvernombud plikter å hindre at andre får adgang eller kjennskap til det de i forbindelse med utførelsen av sine oppgaver får vite om

a) noens personlige forhold

b) tekniske innretninger, produksjonsmetoder, forretningsmessige analyser og beregninger og forretningshemmeligheter ellers når opplysningene er av en slik art at andre kan utnytte dem i sin egen næringsvirksomhet

c) sikkerhetstiltak etter personvernforordningen artikkel 32

d) enkeltpersoners varsling om overtredelser av loven her.

Taushetsplikten gjelder ikke dersom personvernombudet får samtykke fra den opplysningene gjelder, til å legge dem frem, eller dette er nødvendig for gjennomføring av personvernombudets lovpålagte oppgaver.

Taushetsplikten gjelder også etter at personvernombudet har avsluttet tjenesten eller arbeidet. Opplysninger som nevnt i denne paragraf kan heller ikke utnyttes i egen

§ 19.Forskrifter om plikt til å utpeke personvernombud

Kongen kan gi forskrift om plikt til å utpeke personvernombud.

Avsnitt 4 Personvernombud

Artikkel 37.Utpeking av et personvernombud

1. Den behandlingsansvarlige og databehandleren skal utpeke et personvernombud når

a) behandlingen utføres av en offentlig myndighet eller et offentlig organ, bortsett fra domstoler som opptrer innenfor rammen av sin domsmyndighet,

b) den behandlingsansvarliges eller databehandlerens kjernevirksomhet består av behandlingsaktiviteter som på grunn av sin art, sitt omfang og/eller formål krever regelmessig og systematisk monitorering i stor skala av registrerte, eller

c) den behandlingsansvarliges eller databehandlerens kjernevirksomhet består av behandling i stor skala av særlige kategorier av opplysninger i henhold til artikkel 9 eller personopplysninger om straffedommer og lovovertredelser som nevnt i artikkel 10.

2. Et konsern kan utnevne ett personvernombud, forutsatt at alle virksomhetene har enkel tilgang til vedkommende.

3. Dersom den behandlingsansvarlige eller databehandleren er en offentlig myndighet eller et offentlig organ, kan det utpekes ett personvernombud for flere av nevnte myndigheter eller organer, idet det tas hensyn til deres organisasjonsstruktur og størrelse.

4. I andre tilfeller enn dem nevnt i nr. 1 kan eller, dersom det kreves i unionsretten eller i medlemsstatenes nasjonale rett, skal den behandlingsansvarlige eller databehandleren eller sammenslutninger og andre organer som representerer kategorier av behandlingsansvarlige eller databehandlere, utpeke et personvernombud. Personvernombudet kan handle på vegne av nevnte sammenslutninger og andre organer som representerer behandlingsansvarlige eller databehandlere.

5. Personvernombudet skal utpekes på grunnlag av faglige kvalifikasjoner og særlig på grunnlag av dybdekunnskap om personvernlovgivning og praksis på området samt evne til å utføre oppgavene nevnt i artikkel 39.

6. Personvernombudet kan være en ansatt hos den behandlingsansvarlige eller databehandleren eller utføre oppgavene på grunnlag av en tjenesteavtale.

7. Den behandlingsansvarlige eller databehandleren skal offentliggjøre kontaktopplysningene til personvernombudet og meddele disse til tilsynsmyndigheten.

Artikkel 38.Personvernombudets stilling

1. Den behandlingsansvarlige og databehandleren skal sikre at personvernombudet på riktig måte og i rett tid involveres i alle spørsmål som gjelder vern av personopplysninger.

2. Den behandlingsansvarlige og databehandleren skal støtte personvernombudet i forbindelse med utførelsen av oppgavene nevnt i artikkel 39 ved å stille til rådighet de ressurser som er nødvendig for å utføre nevnte oppgaver, samt gi tilgang til personopplysninger og behandlingsaktiviteter og gjøre det mulig for vedkommende å opprettholde sin dybdekunnskap.

3. Den behandlingsansvarlige og databehandleren skal sikre at personvernombudet ikke mottar instrukser om utførelsen av nevnte oppgaver. Vedkommende skal ikke avsettes eller straffes av den behandlingsansvarlige eller databehandleren for å utføre sine oppgaver. Personvernombudet skal rapportere direkte til det høyeste ledelsesnivået hos den behandlingsansvarlige eller databehandleren.

4. De registrerte kan kontakte personvernombudet angående alle spørsmål om behandling av deres personopplysninger og om utøvelsen av de rettighetene de har i henhold til denne forordning.

5. Personvernombudet skal være bundet av taushetsplikt eller en plikt til konfidensiell behandling av opplysninger ved utførelse av sine oppgaver i samsvar med unionsretten eller medlemsstatenes nasjonale rett.

6. Personvernombudet kan utføre andre oppgaver og ha andre plikter. Den behandlingsansvarlige eller databehandleren skal sikre at nevnte oppgaver eller plikter ikke fører til en interessekonflikt.

Artikkel 39.Personvernombudets oppgaver

1. Personvernombudet skal minst ha følgende oppgaver:

a) informere og gi råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har i henhold til denne forordning, og i henhold til andre av Unionens eller medlemsstatenes bestemmelser om vern av personopplysninger,

b) kontrollere overholdelsen av denne forordning, av andre av Unionens eller medlemsstatenes personvernregler og den behandlingsansvarliges eller databehandlerens personvernretningslinjer, herunder fordeling av ansvar, holdningsskapende tiltak og opplæring av personellet som er involvert i behandlingsaktivitetene, og tilhørende revisjoner,

c) på anmodning gi råd om vurderingen av personvernkonsekvenser og kontrollere gjennomføringen av den i henhold til artikkel 35,

d) samarbeide med tilsynsmyndigheten,

e) fungere som kontaktpunkt for tilsynsmyndigheten ved spørsmål om behandlingen, herunder forhåndsdrøftingene nevnt i artikkel 36, og ved behov rådføre seg med tilsynsmyndigheten om eventuelle andre spørsmål.

2. Personvernombudet skal ved utførelsen av sine oppgaver ta behørig hensyn til risikoene forbundet med behandlingsaktivitetene, idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i.

3.2 Guidelines on Data Protection Officers

Article 29 Data Protection Working Party har utarbeidet en veileder kalt *Guidelines on Data Protection Officers ("DPOs")*, første gang utgitt i desember 2016, og revidert i april 2017 (rev.01). Veilederen er ikke tilgjengelig på norsk, og relevante deler av den engelske versjonen er derfor limt inn under.

2.3. Designation of a single DPO for several organisations

Article 37(2) allows a group of undertakings to designate a single DPO provided that he or she is 'easily accessible from each establishment'. The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects19, the supervisory authority20 but also internally within the organisation, considering that one of the tasks of the DPO is 'to inform and advise the controller and the processor and the employees who carry out processing of their obligations pursuant to this Regulation'.21

In order to ensure that the DPO, whether internal or external, is accessible it is important to make sure that their contact details are available in accordance with the requirements of the GDPR.22

He or she, with the help of a team if necessary, must be in a position to efficiently communicate with data subjects23 and cooperate24 with the supervisory authorities concerned. This also means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned. The availability of a DPO (whether physically on the same premises as employees, via a hotline or other secure means of communication) is essential to ensure that data subjects will be able to contact the DPO.

According to Article 37(3), a single DPO may be designated for several public authorities or bodies, taking account of their organisational structure and size. The same considerations with regard to resources and communication apply. Given that the DPO is in charge of a variety of tasks, the controller or the processor must ensure that a single DPO, with the help of a team if necessary, can perform these efficiently despite being designated for several public authorities and bodies.

2.4. Accessibility and localisation of the DPO

According to Section 4 of the GDPR, the accessibility of the DPO should be effective.

To ensure that the DPO is accessible, the WP29 recommends that the DPO be located within the European Union, whether or not the controller or the processor is established in the European Union.

However, it cannot be excluded that, in some situations where the controller or the processor has no establishment within the European Union25, a DPO may be able to carry out his or her activities more effectively if located outside the EU.

2.5. Expertise and skills of the DPO

Article 37(5) provides that the DPO 'shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39'. Recital 97 provides that the necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed.

Level of expertise

The required level of expertise is not strictly defined but it must be commensurate with the sensitivity, complexity and amount of data an organisation processes. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support. There is also a difference depending on whether the organisation systematically transfers personal data outside the European Union or whether such transfers are occasional. The DPO should thus be chosen carefully, with due regard to the data protection issues that arise within the organisation.

Professional qualities

Although Article 37(5) does not specify the professional qualities that should be considered when designating the DPO, it is a relevant element that DPOs must have expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR. It is also helpful if the supervisory authorities promote adequate and regular training for DPOs.

Knowledge of the business sector and of the organisation of the controller is useful. The DPO should also have a good understanding of the processing operations carried out, as well as the information systems, and data security and data protection needs of the controller.

In the case of a public authority or body, the DPO should also have a sound knowledge of the administrative rules and procedures of the organisation.

Ability to fulfil its tasks

Ability to fulfil the tasks incumbent on the DPO should be interpreted as both referring to their personal qualities and knowledge, but also to their position within the organisation. Personal qualities should include for instance integrity and high professional ethics; the DPO's primary concern should be enabling compliance with the GDPR. The DPO plays a key role in fostering a data protection culture within the organisation and helps to implement essential elements of the GDPR, such as the principles of data processing26, data subjects' rights27, data protection by design and by default28, records of processing activities29, security of processing30, and notification and communication of data breaches.31

DPO on the basis of a service contract

The function of the DPO can also be exercised on the basis of a service contract concluded with an individual or an organisation outside the controller's/processor's organisation. In this latter case, it is essential that each member of the organisation exercising the functions of a DPO fulfils all applicable requirements of Section 4 of the GDPR (e.g., it is essential that no one has a conflict of interests). It is equally important that each such member be protected by the provisions of the GDPR (e.g. no unfair termination of service contract for activities as DPO but also no unfair dismissal of any individual member of the organisation carrying out the DPO tasks). At the same time, individual skills and strengths can be combined so that several individuals, working in a team, may more efficiently serve their clients.

For the sake of legal clarity and good organisation and to prevent conflicts of interests for the team members, it is recommended to have a clear allocation of tasks within the DPO team and to assign a single individual as a lead contact and person 'in charge' for each client. It would generally also be useful to specify these points in the service contract.

(…)

3 Position of the DPO

3.1. Involvement of the DPO in all issues relating to the protection of personal data

Article 38 of the GDPR provides that the controller and the processor shall ensure that the DPO is 'involved, properly and in a timely manner, in all issues which relate to the protection of personal data'.

It is crucial that the DPO, or his/her team, is involved from the earliest stage possible in all issues relating to data protection. In relation to data protection impact assessments, the GDPR explicitly provides for the early involvement of the DPO and specifies that the controller shall seek the advice of the DPO when carrying out such impact assessments.33 Ensuring that the DPO is informed and consulted at the outset will facilitate compliance with the GDPR, promote a privacy by design approach and should therefore be standard procedure within the organisation's governance. In addition, it is important that the DPO be seen as a discussion partner within the organisation and that he or she be part of the relevant working groups dealing with data processing activities within the organisation.

Consequently, the organisation should ensure, for example, that:

- ✓ The DPO is invited to participate regularly in meetings of senior and middle management.
- ✓ His or her presence is recommended where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice.
- ✓ The opinion of the DPO must always be given due weight. In case of disagreement, the WP29 recommends, as good practice, to document the reasons for not following the DPO's advice.
- ✓ The DPO must be promptly consulted once a data breach or another incident has occurred.

Where appropriate, the controller or processor could develop data protection guidelines or programmes that set out when the DPO must be consulted.

3.2. Necessary resources

Article 38(2) of the GDPR requires the organisation to support its DPO by 'providing resources necessary to carry out [their] tasks and access to personal data and processing operations, and to maintain his or her expert knowledge'. The following items, in particular, are to be considered:

- ✓ Active support of the DPO's function by senior management (such as at board level).
- ✓ Sufficient time for DPOs to fulfil their duties. This is particularly important where an internal DPO is appointed on a part-time basis or where the external DPO carries out data protection in addition to other duties. Otherwise, conflicting priorities could result in the DPO's duties being neglected. Having sufficient time to devote to DPO tasks is paramount. It is a good practice to establish a percentage of time for the DPO function where it is not performed on a full-time basis. It is also good practice to determine the time needed to carry out the function, the appropriate level of priority for DPO duties, and for the DPO (or the organisation) to draw up a work plan.
- ✓ Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate.
- ✓ Official communication of the designation of the DPO to all staff to ensure that their existence and function are known within the organization.
- ✓ Necessary access to other services, such as Human Resources, legal, IT, security, etc., so that DPOs can receive essential support, input and information from those other services.
- ✓ Continuous training. DPOs must be given the opportunity to stay up to date with regard to developments within the field of data protection. The aim should be to constantly increase the level of expertise of DPOs and they should be encouraged to participate in training courses on data protection and other forms of professional development, such as participation in privacy fora, workshops, etc.

- ✓ Given the size and structure of the organization, it may be necessary to set up a DPO team (a DPO and his/her staff). In such cases, the internal structure of the team and the tasks and responsibilities of each of its members should be clearly drawn up. Similarly, when the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the tasks of a DPO as a team, under the responsibility of a designated lead contact for the client.

In general, the more complex and/or sensitive the processing operations, the more resources must be given to the DPO. The data protection function must be effective and sufficiently well-resourced in relation to the data processing being carried out.

3.3. Instructions and 'performing their duties and tasks in an independent manner'

Article 38(3) establishes some basic guarantees to help ensure that DPOs are able to perform their tasks with a sufficient degree of autonomy within their organisation. In particular, controllers/processors are required to ensure that the DPO 'does not receive any instructions regarding the exercise of [his or her] tasks.' Recital 97 adds that DPOs, 'whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner'.

This means that, in fulfilling their tasks under Article 39, DPOs must not be instructed how to deal with a matter, for example, what result should be achieved, how to investigate a complaint or whether to consult the supervisory authority. Furthermore, they must not be instructed to take a certain view of an issue related to data protection law, for example, a particular interpretation of the law.

The autonomy of DPOs does not, however, mean that they have decision-making powers extending beyond their tasks pursuant to Article 39.

The controller or processor remains responsible for compliance with data protection law and must be able to demonstrate compliance.34 If the controller or processor makes decisions that are incompatible with the GDPR and the DPO's advice, the DPO should be given the possibility to make his or her dissenting opinion clear to the highest management level and to those making the decisions. In this respect, Article 38(3) provides that the DPO 'shall directly report to the highest management level of the controller or the processor'. Such direct reporting ensures that senior management (e.g. board of directors) is aware of the DPO's advice and recommendations as part of the DPO's mission to inform and advise the controller or the processor. Another example of direct reporting is the drafting of an annual report of the DPO's activities provided to the highest management level.

3.4. Dismissal or penalty for performing DPO tasks

Article 38(3) requires that DPOs should 'not be dismissed or penalised by the controller or the processor for performing [their] tasks'.

This requirement strengthens the autonomy of DPOs and helps ensure that they act independently and enjoy sufficient protection in performing their data protection tasks.

Penalties are only prohibited under the GDPR if they are imposed as a result of the DPO carrying out his or her duties as a DPO. For example, a DPO may consider that a particular processing is likely to result in a high risk and advise the controller or the processor to carry out a data protection impact assessment but the controller or the processor does not agree with the DPO's assessment. In such a situation, the DPO cannot be dismissed for providing this advice.

Penalties may take a variety of forms and may be direct or indirect. They could consist, for example, of absence or delay of promotion; prevention from career advancement; denial from benefits that other employees receive. It is not necessary that these penalties be actually carried out, a mere threat is sufficient as long as they are used to penalise the DPO on grounds related to his/her DPO activities.

As a normal management rule and as it would be the case for any other employee or contractor under, and subject to, applicable national contract or labour and criminal law, a DPO could still be dismissed legitimately for reasons other than for performing his or her tasks as a DPO (for instance, in case of theft, physical, psychological or sexual harassment or similar gross misconduct).

In this context it should be noted that the GDPR does not specify how and when a DPO can be dismissed or replaced by another person. However, the more stable a DPO's contract is, and the more guarantees

exist against unfair dismissal, the more likely they will be able to act in an independent manner. Therefore, the WP29 would welcome efforts by organisations to this effect.

3.5. Conflict of interests

Article 38(6) allows DPOs to 'fulfil other tasks and duties'. It requires, however, that the organisation ensure that 'any such tasks and duties do not result in a conflict of interests'.

The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests. This entails in particular that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.

As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.

Depending on the activities, size and structure of the organisation, it can be good practice for controllers or processors:

- ✓ to identify the positions which would be incompatible with the function of DPO
- ✓ to draw up internal rules to this effect in order to avoid conflicts of interests
- ✓ to include a more general explanation about conflicts of interests
- ✓ to declare that their DPO has no conflict of interests with regard to its function as a DPO, as a way of raising awareness of this requirement
- ✓ to include safeguards in the internal rules of the organisation and to ensure that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests. In this context, it should also be borne in mind that conflicts of interests may take various forms depending on whether the DPO is recruited internally or externally

4 Tasks of the DPO

4.1. Monitoring compliance with the GDPR

Article 39(1)(b) entrusts DPOs, among other duties, with the duty to monitor compliance with the GDPR. Recital 97 further specifies that DPO 'should assist the controller or the processor to monitor internal compliance with this Regulation'.

As part of these duties to monitor compliance, DPOs may, in particular:

- ✓ collect information to identify processing activities
- ✓ analyse and check the compliance of processing activities
- ✓ inform, advise and issue recommendations to the controller or the processor

Monitoring of compliance does not mean that it is the DPO who is personally responsible where there is an instance of non-compliance. The GDPR makes it clear that it is the controller, not the DPO, who is required to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation' (Article 24(1)). Data protection compliance is a corporate responsibility of the data controller, not of the DPO.

4.2. Role of the DPO in a data protection impact assessment

According to Article 35(1), it is the task of the controller, not of the DPO, to carry out, when necessary, a data protection impact assessment ('DPIA'). However, the DPO can play a very important and useful role in assisting the controller. Following the principle of data protection by design, Article 35(2) specifically requires that the controller 'shall seek advice' of the DPO when carrying out a DPIA. Article 39(1)(c), in turn, tasks the DPO with the duty to 'provide advice where requested as regards the [DPIA] and monitor its performance pursuant to Article 35'.

The WP29 recommends that the controller should seek the advice of the DPO, on the following issues, amongst others 35:

- ✓ whether or not to carry out a DPIA
- ✓ what methodology to follow when carrying out a DPIA
- ✓ whether to carry out the DPIA in-house or whether to outsource it
- ✓ what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
- ✓ whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR

If the controller disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account36.

The WP29 further recommends that the controller clearly outline, for example in the DPO's contract, but also in information provided to employees, management (and other stakeholders, where relevant), the precise tasks of the DPO and their scope, in particular with respect to carrying out the DPIA.

4.3. Cooperating with the supervisory authority and acting as a contact point

According to Article 39(1)(d) and (e), the DPO should 'cooperate with the supervisory authority' and 'act as a contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter'.

These tasks refer to the role of 'facilitator' of the DPO mentioned in the introduction to these Guidelines. The DPO acts as a contact point to facilitate access by the supervisory authority to the documents and information for the performance of the tasks mentioned in Article 57, as well as for the exercise of its investigative, corrective, authorisation, and advisory powers mentioned in Article 58. As already mentioned, the DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law (Article 38(5)). However, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority. Article 39(1)(e) provides that the DPO can consult the supervisory authority on any other matter, where appropriate.

4.4. Risk-based approach

Article 39(2) requires that the DPO 'have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing'.

This article recalls a general and common sense principle, which may be relevant for many aspects of a DPO's day-to-day work. In essence, it requires DPOs to prioritise their activities and focus their efforts on issues that present higher data protection risks. This does not mean that they should neglect monitoring compliance of data processing operations that have comparatively lower level of risks, but it does indicate that they should focus, primarily, on the higher-risk areas.

This selective and pragmatic approach should help DPOs advise the controller what methodology to use when carrying out a DPIA, which areas should be subject to an internal or external data protection audit, which internal training activities to provide to staff or management responsible for data processing activities, and which processing operations to devote more of his or her time and resources to.

36 Article 24(1) provides that 'taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the

controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary'.

4.5. Role of the DPO in record-keeping

Under Article 30(1) and (2), it is the controller or the processor, not the DPO, who is required to 'maintain a record of processing operations under its responsibility' or 'maintain a record of all categories of processing activities carried out on behalf of a controller'.

In practice, DPOs often create inventories and hold a register of processing operations based on information provided to them by the various departments in their organisation responsible for the processing of personal data. This practice has been established under many current national laws and under the data protection rules applicable to the EU institutions and bodies.37

Article 39(1) provides for a list of tasks that the DPO must have as a minimum. Therefore, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the record of processing operations under the responsibility of the controller or the processor. Such a record should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.

In any event, the record required to be kept under Article 30 should also be seen as a tool allowing the controller and the supervisory authority, upon request, to have an overview of all the personal data processing activities an organisation is carrying out. It is thus a prerequisite for compliance, and as such, an effective accountability measure.

(...)

5 ANNEX - DPO GUIDELINES: WHAT YOU NEED TO KNOW

The objective of this annex is to answer, in a simplified and easy-to-read format, some of the key questions that organisations may have regarding the new requirements under the General Data Protection Regulation (GDPR) to appoint a DPO.

(…)

8. What are the professional qualities that the DPO should have?
The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil his or her tasks.

The necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support.

Relevant skills and expertise include:
- ✓ expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR
- ✓ understanding of the processing operations carried out
- ✓ understanding of information technologies and data security
- ✓ knowledge of the business sector and the organisation
- ✓ ability to promote a data protection culture within the organisation

Source: Article 37(5) of the GDPR

Kontakt oss

Ole Willy Fundingsrud

Oppdragsansvarlig

T +47 40 63 96 92

E ole.willy.fundingsrud@kpmg.no

Nils Harald Børve

Fagansvarlig

T +47 40 63 97 02

E nils.harald.borve@kpmg.no

Veronica Storlid Kvinge

Prosjektleder

T +47 95 85 50 55

E veronica.kvinge@kpmg.no

kpmg.no