
Saksnr: 2021/45338-1
Saksbehandlar: Knut Roald
Dato: 27.08.2021

Til: Kontrollutvalet

Frå: Fung. Personvernombod

Orientering om arbeid med etterleving av personvernregelverket i Vestland fylkeskommune

Kontrollutvalet vart sist orientert om status for arbeidet med personvern på møte 15.02.2021.

Den første delen av dette notatet er ein status pr 31.08.21 med referanse til arbeidet i perioden februar – august 2021 og forslag til tiltak. Den siste delen av notatet er skisser til ein handlingsplan for arbeid med personvern i dei månadene som er att i 2021 og vidare i 2022.

Status – etterleving av personvernregelverket pr 31.08.2021

Personvernforordninga fastslår at den som er behandlingsansvarleg skal påvise at prinsippa for behandling av personopplysningar vert overhalde¹. Dei andre føresegnene i personvernforordninga står opp under dette kravet. For å gje tilbakemelding på status for etterleving av personvernregelverket, er det i det vidare tatt utgangspunkt i aktuelle føresegner som stiller krav til VLFK som behandlingsansvarleg.

Tabellen under gjev oversikt over status for etterleving pr 31.08.2021.

Artikkel	Krav	Status	Vurdering
12-14	Klar og tydeleg informasjon	VLFK har personvernerklæringar på ulike områder. Det er behov for revisjon og å sjå desse i samanheng.	Kravet er oppfylt, men det er naudsynt med revisjon av erklæringane for å sikre at dei er oppdatert og harmonisert.
15-22	Rett til innsyn	VLFK har mottatt to førespurnader om innsyn i perioden. Det er laga utkast til rutine for handsaming av krav frå den registrerte. Det er også utarbeida elektronisk kravsskjema.	Krav om innsyn mv. vert tatt hand om i dag. VLFK oppfyller kravet. Det er naudsynt å slutføre arbeidet med rutine og elektronisk skjema.
24	Internkontroll	Det er p.t. ikkje etablert system for overordna internkontroll på personvernområdet. Det er utarbeida internkontroll dokumentasjon i kvalitetssystemet. Det er likevel behov for å strukturere og	Det bør utarbeidast ein handlingsplan for arbeid med personvern i VLFK med formål å etablere overordna internkontroll. I dette bør organisering av personvernarbeidet og

¹ Personvernforordninga artikkel 5 nr 2.

		<p>harmonisere denne dokumentasjonen.</p> <p>Det er gjennomført nanoopplæring innfor fagområdet informasjonssikkerheit i regi av informasjonssikkerheitsrådgevar. Denne opplæringa dekker ikkje alle tema som er relevant for personvern.</p>	<p>personverndokumentasjon vurderast og oppdaterast.</p> <p>Det bør utarbeidast ein plan for informasjon og opplæring innfor fagområdet personvern.</p>
25	Innebygd personvern	Den sentrale innkjøpsseksjonen har krav om innebygd personvern i sine innkjøpsprosedyrar.	Det bør etablerast system for å dokumentere at relevant personell har kunnskap om krav til innebygd personvern. Eksempelvis gjennom kvalitetssystemet eller Dossier
28	Databehandlaravtalar	<p>VLFK har ikkje noko oversikt som viser at det er inngått databehandlaravtalar for behandlingar kor dette er eit krav.</p> <p>Den sentrale innkjøpsseksjonen har krav om databehandlaravtalar i sine innkjøpsprosedyrar.</p> <p>Det er ikkje dokumentert at andre einingar som gjer innkjøp har dei same krava.</p>	<p>Oversikt over inngåtte databehandlaravtalar bør gjerast i samanheng med kartlegging og utfylling av protokoll for behandling av personopplysningar.</p> <p>Einingar som arbeider med innkjøp og elles samarbeider med eksterne parter som kan definerast som databehandlar, må få informasjon og opplæring.</p>
30	Protokoll over behandlingsaktivitetar	<p>Pt. har ikkje VLFK oversikt over alle behandlingsaktivitetar i verksemda.</p> <p>Etter Deloitte-rapporten i november 2020 bad personvernombodet personvernkoordinatorane om å sende inn behandlingsprotokoll for sine einingar. P.t. har 49 av 70 einingar levert protokoll, (70 %).</p> <p>Personvernombodet og informasjonssikkerheitsrådgevar har gått gjennom protokollane. Det er varierende kvalitet på desse, men arbeidet gjev godt grunnlag for kartlegging. Kartlegging av behandlingar og dataflyt i OPK starta i juni. Det er gjennomført eit møte med tannhelse for å kartlegge dataflyt/behandlingar i denne eininga.</p>	Det er behov for å fortsette arbeidet med å kartlegge behandlingsaktivitetar pr eining og utarbeide protokollar.
32	Personopplysnings-sikkerheit	Det vises til eiga rapportering for området informasjonssikkerheit.	I perioden har det vore tett samarbeid mellom personvernrådgevar/ombod og informasjonssikkerheitsrådgevar. Det er naudsynt

			at dette samarbeidet fortsett og vert styrka i framtida.
32	Avvik	Det er registrert ni avvik på informasjonssikkerheit og personvern i perioden februar - august.	Det er truleg fleire avvik som ikkje vert melde i kvalitetssystemet. Og det kan være ulike årsaker til dette. Aktuelt tiltak er å informera, oppfordra og gje opplæring om avvikshandsaming i dei ulike einingane. I dette arbeidet har leiarane ei viktig rolle.
34 og 35	Melding til Datatilsynet og varsling av den registrerte	Det er meldt frå om to avvik til Datatilsynet i perioden. Sakshandsaminga er avslutta med generell tilråding. I eit høve har VLFK varsla den registrerte om brot på personopplysningssikkerheita.	
35	Vurdering av personvern-konsekvensar (DPIA)	Det er ikkje gjennomført vurdering av personvernkonsekvensar i perioden. Ved fleire høve er det gjennomført ROS-vurderingar i regi av informasjonssikkerheits-rådgjevar. Det er utarbeida skjema for vurdering av behov for DPIA. Skjemaet bygger på tilråding frå WP29-gruppa ² og er distribuert til personvernkoordinatorane.	Aktuelt tiltak er å informera, oppfordra og gje opplæring om krav til DPIA i dei ulike einingane.
37	Personvernombod	VLFK har utpeikt personvernombod Ombodet og personvernrådgjevar er for tida same person. Rolla som ombod er tildelt førebels på ubestemt tid.	VLFK er ein stor og kompleks organisasjon. Det bør etablerast eit fagmiljø for informasjonssikkerheit og personvern. Personvernombodet bør være knytt til dette fagmiljøet. Aktuell referanse er organiseringa av arbeidet med personvern og informasjonssikkerheit i Bergen kommune.
44	Overføring av opplysningar til land utafor EØS	VLFK gjer bruk av skytjenester og overfører ved fleire høve personopplysningar til land utanfor EØS. Truleg overfører VLFK opplysningar utan at EDPB ³ sitt krav til vern er ivaretatt. I perioden har det vore gjennomført fleire innkjøp kor dette har vore tema.	Det bør utarbeidast ein rettleiar til korleis VLFK skal overhalde krava som gjeld for overføring av opplysningar til land utanfor EU. Aktuelle einingar bør få informasjon og opplæring.

² WP29-gruppa gav personvernråd til EU før oppretting av det europeiske datatilsynet.

³ [European Data Protection Board](#) (Det europeiske datatilsynet.)

		<p>Personvernombodet har også oversendt notat til fylkeskommunedirektøren med anbefaling.</p> <p>EDPB kom før sumaren med rettleiing om problemstillinga. Datatilsynet arbeider fortida med eiga rettleiing.</p>	
--	--	--	--

Skisse til handlingsplan og prosess

Under er skisse til handlingsplan, med utgangspunkt i forslag til tiltak i tabellen over:

1. Kartlegging og behandlingsprotokoll
 Kartlegging med formål å få ei oversikt over dataflyt og behandlingar pr eining i VLFK. Kartlegging gjev grunnlag for utarbeiding av behandlingsprotokollar pr eining. Kartlegging og behandlingsprotokoll gjev grunnlag for organisering og internkontroll.

 Kartlegging er starta opp i OPK og Tannhelse og fortsett hausten 2021 og våren 2022. Der det er gjort kartlegging i 2028, vil den bli lagt til grunn og oppdatert. Målet er at alle avdelingane i VLFK skal kartleggast.
2. Organisering
 Utgangspunktet er at dei som er ansvarleg for arbeidsprosessane og dataflyt er nærast til å avdekke og følgje opp risiko. Organisering av internkontrollarbeidet og utarbeiding av dokumentasjon må ha dette som utgangspunkt. Organisering bør vurderast etter at kartlegging er gjennomført.

 Det er gjeve innspel til organisering av arbeid med informasjonssikkerheit og personvern i VLFK. Det vert arbeidd vidare med dette hausten 2021. Kartlegginga kan også avdekke behov som kan verke inn på forslag til organisering.
3. Dokumentasjon
 Styrande, gjennomførande og kontrollerande dokumentasjon må strukturerast og harmoniserast. Det bør vera eit skilje mellom overordna dokumentasjon som gjeld for alle og dokumentasjon som gjeld for den enkelte arbeidsprosess/flyt eller eining. Dokumentasjon tilpassast dataflyt som eit resultat av kartlegging.

 Strukturering og harmonisering av dokumentasjon på overordna nivå gjennomførast hausten 2021
4. Opplæring
 Opplæring må vera både generell og tilpassa særskilde behov/prosesser. Dokumentasjon på at opplæring er gjennomført kan skje ved bruk av kvalitetssystemet og Dossier.

 Det skal utarbeidast eigen plan for opplæring og informasjon hausten 2021.
5. Årshjul
 Det skal utarbeidast utkast til årshjul for personvernombod, personvernrådgjevar, informasjonssikkerheitsrådgjevar og personvernkoordinatorane hausten 2021.

Utsifting av nøkkelpersonell og innspel til ny organisering

Personvernrådgjevar i 100 % stilling starta arbeidet i fylkeskommunen 09.03.21. Personvernombodet gjekk over til anna stilling i fylkeskommunen frå 01.05.21. Før sumarferien, vart det også klart at informasjonssikkerheitsrådgjevaren har sagt opp si stilling og går over i ny jobb frå 01.10.21.

For tida fungerer personvernrådgjevaren som personvernombod. Det er lyst ut ledig stilling etter informasjonssikkerheitsrådgjevaren. Søknadsfristen var i august.

I april skreiv personvernrådgjevaren eit notat med forslag om å samle fagområda informasjonssikkerheit og personvern i staben i avdeling for strategisk utvikling og digitalisering.