Deloitte.

Forvaltningsrevisjon | Vestland fylkeskommune

Informasjonstryggleik

November 2020

«Forvaltningsrevisjon av informasjonstryggleik»

November 2020

Rapporten er utarbeidd for Vestland fylkeskommune av Deloitte AS.

Deloitte AS
Postboks 6013 Postterminalen,
5892 Bergen
tlf: 55 21 81 00
www.deloitte.no
forvaltningsrevisjon@deloitte.no

Samandrag

Bakgrunn og gjennomføring av forvaltningsrevisjonen

Deloitte har gjennomført ein forvaltningsrevisjon av informasjonstryggleik i Vestland fylkeskommune. Prosjektet blei bestilt av kontrollutvalet i Vestland fylkeskommune i sak PS 51/2020 i møte 11. mai 2020.

Formålet med prosjektet har vore å undersøkje om fylkeskommunen har tilfredsstillande system og rutinar for informasjonstryggleik, og om etablerte standardar og gjeldande lovar og reglar blir følgt innanfor dette området. Det har òg vore eit formål å undersøkje korleis fylkeskommunen praktiserer informasjonstryggleik med omsyn til konfidensialitet og tilgangsstyring, i kva grad fylkeskommunen etterlever sentrale krav i ny personvernlovgjeving, og i kva grad dei tilsette har tilfredsstillande kompetanse knytt til informasjons-tryggleik. I gjennomføringa av forvaltningsrevisjonen har vi gjennomgått relevant dokumentasjon frå fylkeskommunen og gjennomført intervju med tilsette som har ansvar og oppgåver knytt til infomarsjonstryggleik og personvern. Vidare har revisjonen gjennomført ei spørjeundersøking blant eit utval tilsette i fylkeskommunen for å kartleggje i kva grad dei tilsette har kjennskap til og følgjer etablerte rutinar knytt til informasjonstryggleik.

Nedanfor er sentrale vurderingar og konklusjonar frå kvart hovudkapittel kort presentert, før revisjonen sine tilrådingar blir lista opp. Samandraget blir avslutta med ei lesarrettleiing der det går fram korleis rapporten er bygd opp, og kva som er hovudinnhaldet i dei ulike kapitla.

Styringssystem for informasjonstryggleik

Før samanslåinga hadde både Sogn og Fjordane fylkeskommune og Hordaland fylkeskommune investert i å utvikle kvar sine styringssystem for informasjonstryggleik utan at desse blei ferdige før etableringa av Vestland fylkeskommune. Etter etableringa av Vestland fylkeskommune, har tilsvarande arbeid blitt påbegynt ved fleire høve, men grunna mellom anna utskiftingar av personell, pågåande arbeid med å byggje den nye organisasjonen, samt COVID-19-pandemien, var arbeidet med å utarbeide eit styringssystem for informasjonstryggleik framleis ikkje fullført på revisjonstidspunktet.

Dei styrande dokumenta i styringssystemet er i hovudsak ferdige og tilgjengelege for dei tilsette. Revisjonen har ikkje avdekka indikasjonar som tyder på at dei ferdige styrande dokumenta bryt med krava i gjeldande regelverk eller relevante standardar. Dei styrande dokumenta i styringssystemet for informasjonstryggleik blei godkjende relativt nyleg, og arbeidet med å implementere styringssystem i fylkeskommunen var framleis pågåande på revisjonstidspunktet. Både etableringa av Vestland fylkes-kommune og COVID-19-pandemien blir vist til som forklaringar for kvifor styringssystemet ikkje er ferdig utarbeidd og ikkje er ferdig implementert i organisasjonen. Likevel vil revisjonen understreke viktigheita av å ferdigstille og implementere dei styrande dokumenta for informasjonstryggleik, då dette er ein føresetnad for at leiarar og tilsette i heile organisasjonen veit kva mål og strategi fylkeskommunen har for informasjonstryggleik, og vidare for at fylkeskommunen kan etablere ein god informasjonstryggleikspraksis

Rutinar og ansvarsforhold knytt til informasjonstryggleik

Vestland fylkeskommune har, i dei delane av styringssystemet for informasjonstryggleik som so langt er ferdig og tilgjengeleg for tilsette, etablert rutinar som skildrar kva ansvarsforhold og roller som er knytt til arbeidet med informasjonstryggleik. Undersøkingane tyder på at dei formelle rollane ikkje blir praktisert som føresett; t.d. er ikkje alle med systemeigaransvaret klar over at dei har denne rolla og arbeidet med informasjonstryggleik er ikkje i tilstrekkeleg grad forankra på toppnivå i organisasjonen. Revisjonen er merksam på at rollar og ansvar på området relativt nyleg er formalisert. Likevel er det revisjonen si vurdering at Vestland fylkeskommune på revisjonstidspunktet ikkje har ein praksis som sikrar at ansvar og mynde for rollar som er relevante for informasjonstryggleik er både tildelt og kommunisert.

Fleire av rutinane og retningslinjene for informasjonstryggleik i fylkeskommunen sitt styringssystem er etter revisjonen si vurdering eigna til å styrke informasjonstryggleiken i fylkeskommunen, Samtidig viser undersøkinga at det finst fleire rutinar, prosedyrar og retningslinjer som omhandlar informasjonstryggleik og personvern og som er tilgjengelege for tilsette, men som *ikkje* inngår i styringssystemet for informasjonstryggleik; nokre av desse utdaterte, medan andre er feilplasserte og skal etter kvart inngå i styringssystemet. Ein slik situasjon, der styringssystemet ikkje er ferdig, og det parallelt eksisterer rutinedokument som omhandlar same tema, er uheldig. Det er då svært vanskeleg for den enkelte tilsette

å vite kor ein finn rutinar og retningslinjer på området, samt kva av desse som faktisk er gjeldande. Dette kan både føre til at tilsette følgjer rutinar som ikkje gjeld og ikkje finn dei rutinane som gjeld. Konsekvensane av ein slik situasjon kan vere at tilsette ikkje praktiserer informasjonstryggleik i samsvar med gjeldande rutinar, med tilhøyrande risiko for brot på både interne rutinar og ekstern regelverk.

Kontroll og etterprøving av informasjonstryggleik
Styringssystemet inneheld retningslinjer og rutinar for kontroll og etterprøving av informasjonstryggleiken i fylkeskommunen, men desse blir ikkje praktisert; som forklaring viser fylkeskommunen til at styrings-systemet ikkje er ferdig, og at dei delane av styringssystemet som er implementert, blei det relativt nyleg. Revisjonen vil i den samanheng understreke viktigheita av kontroll og etterprøving for å sikre god informasjonstryggleik.

Sikring av konfidensialitet

Vestland fylkeskommune har gjort både organisatoriske og tekniske tiltak for sikring av konfidensialitet. Mellom anna har fylkeskommunen langt på veg sett i verk tilstrekkelege tiltak for å sikre at konfidensiell informasjon kan bli *lagra* trygt. Vidare er det gjennom styringssystemet for informasjonstryggleik stilt krav om at konfidensiell informasjon som *ikkje* blir lagra trygt, skal krypterast. Det er ikkje utarbeidd rutinar eller prosedyrar for korleis slik kryptering skal skje, noko revisjonen meiner er uheldig, då det kan bety at tilsette som lagrar konfidensiell informasjon utanfor sikker sone, ikkje er sett i stand til å ivareta kravet om at opplysningane då skal krypterast. Følgjeleg er det risiko for at konfidensielle opplysningar i Vestland fylkeskommune som ikkje blir lagra trygt, heller ikkje blir kryptert.

Fylkeskommune har vidare fleire retningslinjer og rutinar som er eigna til å bidra til å hindre uautorisert innsyn i konfidensielle opplysningar. Funn i undersøkinga tyder på at desse ikkje alltid blir etterlevd, og det er følgjeleg revisjonen si vurdering at fylkeskommunen ikkje i tilstrekkeleg grad hindrar uautorisert innsyn i konfidensielle opplysningar. Revisjonen vil særleg peike på viktigheita av at fylkeskommunen sine tryggleiksreglar knytt til e-postbruk blir etterlevd. Sannsynet for at konfidensielle opplysningar kjem på avvege om slike blir sendt per e-post er relativt høg, og konsekvensane kan vere negative både for fylkeskommunen og for dei opplysningane angår. Vidare er det svært viktig at dei tilsette praktiserer trygg e-postbruk når det gjeld vedlegg og lenkar; konsekvensane av at berre éin tilsett trykkar på ein falsk lenke eller opnar eit vondsinna vedlegg kan vere svært alvorlege for både fylkeskommunen sjølv, og for fylkeskommunen sine tenestemottakarar.

Tilgangsstyring

Vestland fylkeskommune har etablert rutinar for tilgangsstyring og for å hindre uautorisert tilgang til informasjonssystema. Revisjonen har ikkje avdekka noko som tilseier at desse rutinane ikkje er formålstenlege eller at dei ikkje er eigna til å hindre uautorisert tilgang til informasjonssystema. Fylkes-kommunen har òg ein praksis på desse områda som langt på veg er automatisert, og som slik bidreg til å hindre uautorisert tilgang til mange av informasjonssystema. Manglande automatisering for nokre av informasjonssystema gjev likevel auka risiko for svikt i tilgangsstyringa, noko som òg medfører risiko for uautorisert tilgang til informasjonssystema. Vår vurdering er difor at Vestland fylkeskommune ikkje fullt ut har system, rutinar og praksis som hindrar uautorisert tilgang til informasjonssystema.

Svakheitene knytt til å hindre uautorisert tilgang til informasjonssystema er særleg knytt til prosessane for utmelding av tilsette i informasjonssystema. Revisjonen si vurdering er at rutinane for å sikre at tilsette som sluttar eller bytter avdeling internt i Vestland fylkeskommune mistar tilgangar dei ikkje lenger har tenestleg behov for, berre i nokon grad er tilfredsstillande. Dette fordi tilgangsstyringa for nokre av informasjonssystema krev manuell operasjonar for å avslutte tilgangen, noko som aukar risikoen for at tilsette som endrar stilling eller som har slutta i fylkeskommunen likevel beheld tilgangar dei ikkje treng.

Fylkeskommunen gjennomgår jamleg tildelte tilgangar til dei mest kritiske informasjonssystema, noko som bidreg til å hindre uautoriserte tilgangar. Dette skjer likevel ikkje i alle informasjonssystema. Vidare er det systemeigarane i Vestland fylkeskommune som har ansvaret for tilgangsstyringa i sine informasjonssystem og som skal gjennomgå tildelte tilgangar. Ikkje alle systemeigarane er klare over kva ansvar dei har. Samla gjev dette risiko for uautorisert tilgang til informasjonssystema.

For å bøte på ein slik risiko, skal brukte tilgangar i informasjonssystema loggførast, og desse loggane skal gjennomgåast. Vestland fylkeskommune har ikkje formelle rutinar for logging av brukte tilgangar i informasjonssystema, men slik logging skjer likevel i praksis i nokre av informasjonssystema, og for nokre av dei igjen blir loggane gjennomgått og kontrollert jamleg. Revisjonen meiner manglande rutinar – og

eventuelt manglande moglegheit – for loggføring av brukte tilgangar i fylkeskommune sine informasjons-system er uheldig. Det er òg uheldig om ikkje brukte tilgangar blir logga i alle systema som har moglegheit for det. Manglande loggføring av brukte tilgangar gjer at det ikkje er mogleg å avdekke eventuell uautorisert bruk av systema. Vidare meiner revisjonen at manglande praksis for å hente ut tilgangslogger frå system der slike blir eller kan produserast, også reduserer sannsynet for at eventuelle uautorisert bruk av desse systema blir avdekt.

Etterleving av sentrale krav i personvernlovgjevinga

Personvernombod

Utskiftingar av personell og vakansar har hatt konsekvensar for Vestland fylkeskommune sitt arbeid med etterleving av personvernforordninga som tredde i kraft i 2018; mellom anna har ulike personar på ulike tidspunkt vore konstituert i rolla som personvernombod. Vestland fylkeskommune tilsette eit personvernombod i 50 % 17. august 2020, med tilhøyrande ansvar og oppgåver. Revisjonen har ikkje avdekt noko som indikerer at mandatet til personvernombodet i Vestland fylkeskommune ikkje oppfyller krava i artikkel 39 i personvernforordringa. Fylkeskommunen har vidare stillingar som supplerer rolla til personvernombodet (personvernrådgjevar og IKT-sikkerheitsrådgjevar).

Protokoll over behandlingsaktivitetar av personopplysningar og databehandlaravtalar

Vestland fylkeskommune stiller gjennom sitt styringssystem for informasjonstryggleik krav om at det skal bli ført protokoll over behandlingar av personopplysningar i samsvar med regelverket. Fylkeskommunen har òg utarbeidd utkast til rutinar for korleis delar av dette arbeidet skal gjennomførast, samt malar for slike protokollar. Fylkeskommunen har vidare begynt arbeidet med å føre slik protokoll over behandlingar av personopplysningar. Dette arbeidet var på revisjonstidspunktet ikkje ferdig. Fylkeskommunen bryt slik med kravet i personvernforordninga artikkel 30 nr. 1, om å føre protokoll over behandlingsaktivitetar av personopplysningar.

Vestland fylkeskommune har vidare etablert skriftlege rutinar for inngåing av databehandlaravtalar, men har ikkje fullstendig oversikt over kva databehandlaravtalar som er inngått. Følgjeleg har fylkeskommunen heller ikkje oversikt over kva databehandlaravtalar som manglar. Det er pågåande arbeid med å etablere slik oversikt. På revisjonstidspunktet meiner revisjonen likevel det er høg risiko for at fylkeskommunen ikkje oppfyller kravet i personvernforordninga artikkel 28 nr. 3, om å ha skriftlege avtalar med alle som behandlar personopplysningar på vegner av fylkeskommunen.

Personvernerklæring

Vestland fylkeskommune har fleire personvernerklæringar tilgjengeleg for publikum på sine nettsider. Det kjem ikkje fram informasjon som tyder på at desse ikkje er i samsvar med krava i personvernforordninga artikkel 12 nr. 1. Det er heller ikkje indikasjonar som tyder på at dei andre personvernerklæringane som er undersøkt (på enkelte vidaregåande skuler) ikkje er i samsvar med krava i personvernforordninga. Det er likevel uheldig at desse har kontaktinformasjon til eit personvernombod som ikkje lenger er tilsett i fylkeskommunen, og elles har innhald som viser til dei førre fylkeskommunane.

Risikovurderingar knytt til handsaming av personopplysningar

Vestland fylkeskommune har etablert rutinar for gjennomføring av risikovurderingar knytt til behandling av personopplysningar og personvernkonsensvurderingar (DPIA), og har vidare ytterlegare rutinar under utarbeiding. Undersøkinga viser òg at det har blitt gjennomført nokre slike risikovurderingar, men at desse i hovudsak har vært gjort for behandlingar av personopplysningar i nye system; for eksisterande system har det ikkje eller berre i nokon grad blitt gjort risikovurderingar knytt til behandling av personopplysningar eller personvernkonsekvensvurderingar. Vidare kjem det fram at fylkeskommunen ikkje har noko risikoregisert med oversikt over kva system og behandlingar av personopplysningar som er risikovurdert, og kva som ikkje er risikovurdert. Revisjonen er merksam på at det har blitt gjennomført fleire risikovurderingar, og at fylkeskommunen har desse samla. Likevel meiner vi at det er uheldig at fylkeskommunen ikkje har oversikt over kva som er gjort og kva som står att med omsyn til risikovurderingar av behandlingar av personopplysningar.

Avvik og avviksmelding til Datatilsynet

Vestland fylkeskommune har etablert rutinar for avviksmelding som mellom anna seier at personvernavvik skal meldast til Datatilsynet innan 72, timar, slik det er stilt krav om i personvernforordninga. Vestland fylkeskommune har vidare eit avviksystem tilgjengeleg for alle tilsette, og undersøkinga viser at det blir meldt avvik knytt til informasjonstryggleik i dette. Svara i spørjeundersøkinga tyder på at ikkje alle tilsette

i fylkeskommunen veit at dei skal melde avvik knytt til informasjonstryggleik når dei opplever eller observerer slike. Dette gjev risiko for at avvik ikkje blir meldt, og både svara i spørjeundersøkinga, informasjon frå intervju og talet informasjonstryggleiksavvik meldt i avviksystemet tyder på at denne risikoen har gjort seg gjeldande i fylkeskommunen. Revisjonen vil i den samanheng peike på at manglande avviksmeldingar aukar risikoen for at svakheiter i systema ikkje blir retta.

Kompetanse om informasjonstryggleik

Rutinar for opplæring i informasjonstryggleik

Vestland fylkeskommune har gjennom dei delane av styringssystemet for informasjonstryggleik som er ferdig, plassert ansvar og oppgåver knytt til opplæring innanfor informasjonstryggleik. Vidare skal alle tilsette i Vestland fylkeskommune vere informert om grunnleggjande informasjonstryggleikskrav gjennom internt regelverk. Både delane av styringssystemet som er ferdig og det aktuelle regelverket er nyleg utarbeidd og godkjent. Fylkeskommunen er vidare open på at opplæring av tilsette ikkje har blitt prioritert før organisasjonen har gjort ferdig nødvendig dokumentasjon i styringssystemet, og at det difor ikkje har blitt gitt systematisk opplæring på dette området. Det er heller ikkje lagt konkrete planar for korleis slik opplæring skal bli gitt. Resultatet frå spørjeundersøkinga stadfester dette. Det er følgjeleg revisjonen si vurdering at Vestland fylkeskommune ikkje oppfyller krav og anbefalingar knytt til å sikre tilstrekkeleg informasjonstryggleikskompetanse blant dei tilsette gjennom opplæringstiltak.

Kjennskap til retningslinjer og rutinar for informasjonstryggleik

Vestland fylkeskommune har i nokon grad etablert prosedyrar og instruksar som legg til rette for at tilsette skal tileigne seg kunnskap og kompetanse knytt til informasjonstryggleik. Denne dokumentasjonen er nyleg gjort tilgjengeleg for dei tilsette, og ikkje alle tilsette er kjende med innhaldet. Dette kjem mellom anna fram i spørjeundersøkinga. Revisjonen er merksam på at fylkeskommunen er i prosess med å ferdiggjere sitt styringssystem for informasjonstryggleik, og vidare at fylkeskommunen er open på at dei so langt ikkje har blitt gitt systematisk opplæring i informasjonstryggleik til dei tilsette. Revisjonen meiner difor at fylkeskommunen ikkje i tilstrekkeleg grad har sikra tilfredsstillande opplæring av dei tilsette, noko som medfører risiko for brot på regelverk og anbefalingar på området grunna manglande kompetanse.

Dette blir understreka i funna knytt til etterleving av retningslinjer og rutinar for informasjonstryggleik, som viser at retningslinjer og rutinar for informasjonstryggleik ikkje alltid blir etterlevd i Vestland fylkeskommune. Det kjem mellom anna fram at 13,2 % av respondentane sjølve har delt brukarnamn og passord med andre, og nesten 40 % har observert at dette har skjedd blant kollegaar. Sjølv om det i Vestland fylkeskommune er vanleg rutine at tilsette som delar passord med IT-tenesta blir bedne om å endre passordet sitt etterpå, vil revisjonen understreke at det å dele passord med andre ikkje er i samsvar med grunnleggjande prinsipp for informasjonstryggleik eller fylkeskommunen sine eigne retningslinjer, og at dette også gjeld dersom det er IT-tenesta ein deler passordet med.

Basert på funna frå undersøkinga, er det revisjonen si vurdering at dei tilsette i Vestland fylkeskommune i liten grad etterlever retningslinjer og rutinar for informasjonstryggleik. Dette gjev auka risiko for informasjonstryggleiksbrot, og revisjonen meiner fylkeskommunen må gjere tiltak for å sikre etterleving av retningslinjer og rutinar for informasjonstryggleik.

Tilrådingar

Basert på funna i undersøkinga, tilrår revisjonen at Vestland fylkeskommune gjennomfører tiltak for å sikre følgjande:

1. at fylkeskommunen sitt styringssystem blir gjort ferdig og implementert i organisasjonen, og som del av dette sikre at:
   a) ansvarsforhold knytt til informasjonstryggleik blir gjort kjend og etterlevd av dei tilsette
   b) rutinar for informasjonstryggleik blir gjort ferdige, kjende og blir etterlevd av dei tilsette
   c) det blir gjennomført tilstrekkeleg kontroll og etterprøving av informasjonstryggleiken
2. at ansvar og rutinar for å hindre uautorisert innsyn i konfidensielle opplysningar er utfyllande, tydelege og blir etterlevd, og som del av dette gjer tiltak for at tilsette:
   a) praktiserer trygg bruk av e-post, t.d. gjennom nettfiskeforsøk
   b) nyttar sikker sone ved lagring av konfidensielle opplysningar
   c) krypterer konfidensielle opplysningar som ikkje er lagra i sikker sone

3. at ansvar og rutinar for å hindre uautorisert tilgang til informasjonssystema er utfyllande, tydelege og blir etterlevd, og som del av dette gjer tiltak for å:
   a) sikre at tilsette har nødvendige tilgangar
   b) sikre at tilsette ikkje har tilgangar utan at det er tenestleg behov
4. at krava i personvernforordninga blir etterlevde, og som del av dette:
   a) føre protokoll over alle behandlingar av personopplysningar
   b) signere databehandlaravtalar med alle kommunen sine databehandlarar
   c) gjennomføre risikovurderingar knytt til behandlingar av personopplysningar
   d) gjennomføre vurdering av personvernkonsekvensar ved behandlingar av personopplysningar med høg risiko
5. at systemeigarar og andre med ansvar knytt til informasjonstryggleik og personvern mottek tilstrekkeleg opplæring
6. at det blir utarbeidd tilstrekkeleg med informasjon om informasjonstryggleik til dei tilsette, og sikre at dei tilsette får den naudsynte opplæringa for å kunne ivareta informasjonstryggleiken på ein tilfredsstillande måte.

Lesarrettleiing

Kapitla i forvaltningsrevisjonsrapporten har følgjande hovudinnhald:

Kapittel 1: Dette kapittelet er innleiinga til forvaltningsrevisjonsrapporten. Her blir bakgrunn for prosjektet presentert, saman med føremål og problemstillingar. Vidare er det gjort kort greie for den metodiske tilnærminga som er nytta og verifiseringsprosessar som er gjennomførte.

Kapittel 2: Kapittel to er eit bakgrunnskapittel, og inneheld mellom anna litt kort historikk og overordna om status på arbeidet med informasjonstryggleik i Vestland fylkeskommune, samt ein presentasjon av organiseringa av informasjonstryggleiksarbeidet i Vestland fylkeskommune.

Kapittel 3: I kapittel tre, *Styringssystem for informasjonstryggleik*, svarer revisjonen på første hovudproblemstilling. Innleiingsvis blir problemstillinga og revisjonskriterium som er relevante for å svare på problemstillingane presentert. Det blir så sett nærare på om dei styrande dokumenta i styringssystemet er i samsvar med krav og tilrådingar, om det er etablert tydelege ansvarsforhold og rutinar for informasjonstryggleiksarbeidet, samt om det blir gjennomført kontroll og etterprøving av informasjonstryggleiken.

Kapittel 4: I kapittel fire, *Konfidensialitet*, svarer revisjonen på den andre hovudproblemstillinga. Også i dette kapittelet blir problemstilling og relevante revisjonskriterium presentert innleiingsvis. Temaet i kapittelet er korleis fylkeskommunen arbeider for å hindre uautorisert innsyn i konfidensielle opplysningar.

Kapittel 5: I kapittel fem, *Tilgangsstyring,* svarer revisjonen på tredje hovudproblemstilling. Også her blir problemstillingar og relevante revisjonskriterium presentert innleiingsvis. Temaet i kapittelet er om og korleis fylkeskommunen hindrar uautorisert tilgang til informasjonssystema, inkludert med omsyn til inn- og utmelding av tilsette i relevante informasjonssystema, vurdering av om tilsette har riktige tilgangar i informasjonssystema, samt loggføring av brukte tilgangar i informasjonssystema.

Kapittel 6: I kapittel seks, *Personvern*, svarer revisjonen på fjerde hovudproblemstilling. Innleiingsvis blir problemstillinga og relevante revisjonskriterium presentert. I dette kapittelet er temaet etterleving av personopplysningslova, med fokus på om fylkeskommunen etterlever utvalde, grunnleggjande krav i regelverket (om dei har personvernombod og personvernerklæring, førar protokoll over behandlingar av personopplysningar, gjer risikovurderingar av slike behandlingar, og om avvik blir meldt).

Kapittel 7: I kapittel sju, *Kompetanse om informasjonstryggleik*, svarer revisjonen på femte hovud-problemstilling. Som i dei andre problemstillingkapitla, blir også her problemstillingar og relevante revisjonskriterium presentert innleiingsvis. Temaet for kapittelet er dei tilsette i fylkeskommunen sin informasjonstryggleikskompetanse, inkludert om det er etablert rutinar

for å gje tilsette opplæring i informasjonstryggleik, i kva grad har dei tilsette kjennskap til retningslinjer og rutinar for informasjonstryggleik, og i kva grad desse blir følgt.

Kapittel 8: I kapittel åtte, *Konklusjon og tilrådingar*, er revisjonen sine samla konklusjonar presenterte, saman med ei opplisting av tiltak revisjonen meiner at fylkeskommunen bør setje i verk basert på den undersøkinga som er gjennomført.

Innhald

Detaljert innhaldsliste

Figurar

Tabellar

1. Innleiing

1.1 Bakgrunn

Deloitte har gjennomført ein forvaltningsrevisjon av informasjonstryggleik i Vestland fylkeskommune. Prosjektet blei bestilt av kontrollutvalet i Vestland fylkeskommune i sak PS 51/2020 i møte 11. mai 2020.[1]

Prosjektet var prioritert som høvesvis nr. 2 og nr. 6 i dei rullerte planane for forvaltningsrevisjon i Sogn og Fjordane fylkeskommune og Hordaland fylkeskommune.

1.2 Formål og problemstillingar

Formålet med prosjektet har vore å undersøkje om fylkeskommunen har tilfredsstillande system og rutinar for informasjonstryggleik, og om etablerte standardar og gjeldande lovar og reglar blir følgt innanfor dette området. Det har òg vore eit formål å undersøkje korleis fylkeskommunen praktiserer informasjonstryggleik med omsyn til konfidensialitet og tilgangsstyring, i kva grad fylkeskommunen etterlever sentrale krav i ny personvernlovgjeving, og kva kompetanse dei tilsette har på området.

Med bakgrunn i formålet er det utarbeidd følgjande problemstillingar som har blitt undersøkt:

1. I kva grad har Vestland fylkeskommune etablert styringssystem for informasjonstryggleik som tilfredsstillar krav i sentrale føresegner?
   a) Er styrande dokument for informasjonstryggleik i samsvar med krav i regelverket?
   b) Er det etablert klåre rutinar og ansvarsforhold knytt til informasjonstryggleik?
   c) Har fylkeskommunen system for kontroll og etterprøving av informasjonstryggleik, og blir slik kontroll og etterprøving gjennomført?
2. I kva grad har Vestland fylkeskommune etablert rutinar for sikring av konfidensialitet, og i kva grad blir disse etterlevd? Under dette:
   a) Hindre uautorisert innsyn i konfidensielle opplysningar
   b) Sikker sone for lagring av konfidensielle opplysningar
   c) Kryptering av konfidensielle opplysningar
3. I kva grad har Vestland fylkeskommune etablert rutinar for tilgangsstyring, og i kva grad blir disse etterlevd? Under dette:
   a) Hindre uautorisert tilgang til informasjonssystema
   b) Inn- og utmelding av tilsette i relevante informasjonssystema
   c) Vurdering av om tilsette har riktige tilgangar i informasjonssystema
   d) Loggføring av brukte tilgangar i informasjonssystema
4. I kva grad etterlever Vestland fylkeskommune sentrale krav i personvernlovgjevinga?
   a) Har fylkeskommunen eit personvernombod med tilhøyrande ansvar og oppgåver som tilfredsstillar krava regelverket?
   b) Fører fylkeskommunen protokoll over behandlingsaktivitetar av personopplysningar i samsvar med krava i regelverket?
   c) Har fylkeskommunen personvernerklæring som følgjer krava i regelverket?
   d) I kva grad blir det gjort risiko- og konsekvensvurderingar av handsaming av personopplysningar der det er krav om dette?
   e) I kva grad har fylkeskommunen oversikt over avvik knytt til personvern, og i kva grad blir slike avvik meldt til Datatilsynet?
5. I kva grad har dei tilsette i fylkeskommunen tilstrekkeleg kompetanse om informasjonstryggleik?
   a) Er det etablert rutinar for å gje tilsette opplæring i informasjonstryggleik?
   b) I kva grad har dei tilsette kjennskap til ev. retningslinjer og rutinar for informasjonstryggleik?
   c) I kva grad blir ev. retningslinjer og rutinar for informasjonstryggleik følgt?

1.3 Avgrensing

Undersøkinga har primært fokusert på krav stilt til handsaming og sikring av personopplysningar. Personopplysningslova og -forordninga (GDPR) stiller strenge krav til handsaming og sikring av slike

[1] Prosjektplanen blei noko justert i september 2020, jf. sak PS 73/20.

opplysningar, og ein lekkasje av denne typen informasjon kan få store konsekvensar, både for fylkeskommunen og personane som blir råka. Revisjonen har ikkje gjennomført undersøkingar, testingar eller analysar av teknisk konfigurasjon, tryggingstiltak eller operative driftsrutinar.

1.4 Metode

Oppdraget er utført i samsvar med gjeldande standard for forvaltningsrevisjon (RSK 001) og kvalitetssikring er underlagt krava til kvalitetssikring i Deloitte Policy Manual (DPM).

Oppdraget er gjennomført i tidsrommet juni 2020 til november 2020.

1.4.1 Dokumentanalyse

Rettsreglar og fylkeskommunale vedtak har blitt gjennomgått og nytta som revisjonskriterium. Vidare vil informasjon om fylkeskommunen og dokumentasjon på etterleving av interne rutinar, regelverk m.m. bli samla inn og analysert. Innsamla dokumentasjon vil bli vurdert opp mot revisjonskriteria. Dokumentanalysen har blitt gjennomført løypande, slik at også dokument som har blitt utarbeidd under prosjektperioden har blitt analysert.

1.4.2 Intervju

For å få supplerande informasjon til skriftlege kjelder har Deloitte intervjua utvalde personar frå Vestland fylkeskommune som er involvert i eller har ansvar for informasjonstryggleik i ulike delar av organisasjonen. Vi har intervju totalt seks personar. Intervjua blei gjennomført i august 2020.

1.4.3 Spørjeundersøking

Revisjonen har gjennomført ei elektronisk spørjeundersøking blant eit utval tilsette i Vestland fylkeskommune. Formålet med spørjeundersøkinga var å kartleggje i kva grad dei tilsette har kjennskap til og følgjer etablerte rutinar knytt til informasjonstryggleik. Utvalet var vekta og tilfeldig, slik at eit tilfeldig utval tilsette frå flest mogleg einingar blei invitert til å svare på undersøkinga. Responsraten per avdeling og totalt er presentert i tabellen under:

Tabell 1: Responsrate

Avdeling	Tal inviterte	Tal svar	Responsrate
Organisasjon og økonomi	70	47	67,14 %
Strategisk utvikling og digitalisering	104	53	50,96 %
Infrastruktur og veg	56	38	67,86 %
Mobilitet og kollektivtransport	31	24	77,24 %
Innovasjon og næringsutvikling	22	17	77,27 %
Opplæring og kompetanse	222	119	55,60 %
Kultur, idrett og inkludering	39	28	71,79 %
Sum	**544**	**326**	**60 %**

Då variasjonane i svara frå dei ulike delane av organisasjonen er små, er resultata frå spørjeundersøkinga presentert for fylkeskommunen samla i rapporten.

Spørjeundersøkinga blei gjennomført frå slutten av august 2020 til midten av september 2020.

1.4.4 Verifiseringsprosessar

Oppsummering av intervju er sendt til dei som er intervjua for verifisering og det er informasjon frå dei verifiserte intervjureferata som er nytta i rapporten.

Datadelen av rapporten er sendt til fylkesrådmannen for verifisering, og eventuelle faktafeil vil bli retta opp i den endelege versjonen. Høyringsutkast av rapporten er sendt til fylkesrådmannen for uttale. Fylkesrådmannen sin høyringsuttale er å finne i vedlegg 1.

1.5 Revisjonskriterium

Revisjonskriteria er dei krav og forventningar som forvaltningsrevisjonsobjektet skal bli vurdert opp mot. Kriteria er utleia frå autoritative kjelder i samsvar med krava i gjeldande standard for forvaltningsrevisjon. I dette prosjektet er revisjonskriteria i hovudsak henta frå lov om behandling av personopplysningar, eForvaltningsforskrifta og ISO27001:2013. Kriteria er nærare presentert innleiingsvis under kvart tema, og i vedlegg 2 til rapporten.

2. Om tenesteområdet

2.1 Innleiing

Sogn og Fjordane fylkeskommune og Hordaland fylkeskommune blei slått saman til Vestland fylkeskommune frå 1. januar 2020. Samanslåingsprosessen har kravd mykje tid og ressursar for organisasjonen, både før og etter samanslåinga var fullført.[2] Mellom anna har prosessen tatt opp mykje av kapasiteten til IT-avdelingane i både dei gamle fylkeskommunane og den nye fylkeskommunen. Dei tilsette innanfor IT og IKT-tryggleik i Vestland fylkeskommune har arbeidd med å stenge av gamle system og bygge opp nye system, samt innarbeide nyoppretta avdelingar, seksjonar og kompetansemiljø.

Før samanslåinga hadde både Sogn og Fjordane fylkeskommune og Hordaland fylkeskommune investert i å utvikle kvar sine styringssystem for informasjonstryggleik (ISMS),[3] utan at desse blei ferdige. Etter etableringa av Vestland fylkeskommune, har tilsvarande arbeid blitt påbegynt ved fleire høve, men grunna mellom anna utskiftingar av personell er arbeidet med styringssystemet for informasjonstryggleik framleis ikkje fullført. Utskiftingar av personell og vakansar har òg hatt konsekvensar for Vestland fylkeskommune sitt arbeid med etterleving av personvernforordninga som tredde i kraft i 2018; ulike personar har på ulike tidspunkt vore konstituert i rolla som personvernombod (sjå kapittel 6).

I prosessen med etableringa av Vestland fylkeskommune blei det tatt fleire organisatoriske grep med sikte på å leggje til rette for at organisasjonen skal få etablert god informasjonstryggleik (sjå seksjonane 2.2 og 3.4). Mellom anna blei ulike rollar og ansvarsområde knytt til informasjonstryggleik plassert i ulike einingar i fylkeskommune, slik at ein skal sikre tilstrekkeleg uavhengigheit og unngå samanblanding av rollar. Det blei òg arbeidd systematisk med informasjonstryggleik og personvern i samanslåingsprosessen, men dette arbeidet var ikkje heilt ferdig verken organisatorisk eller teknisk då den nye fylkeskommunen formelt blei etablert 1. januar 2020. Arbeidet blei vidare forseinka som følgje av COVID-19, då om lag 600 tilsette – deriblant fleire med sentrale oppgåver knytt til informasjonstryggleik – måtte arbeide frå heimekontor.

I sum har samanslåingsprosessen, COVID-19 og vakansar i sentrale stillingar ført til at Vestland fylkeskommune framleis har ein veg å gå med å gjere ferdig styringssystemet for informasjonstryggleik (sjå kapittel 3), og med å få bygd ein organisasjon med ein moden tryggleikskultur (sjå kapittel 7).

Det blei innført eit nytt kvalitetssystem i organisasjonen 01.01.2020 ved overgangen til Vestland fylkeskommune.[4]

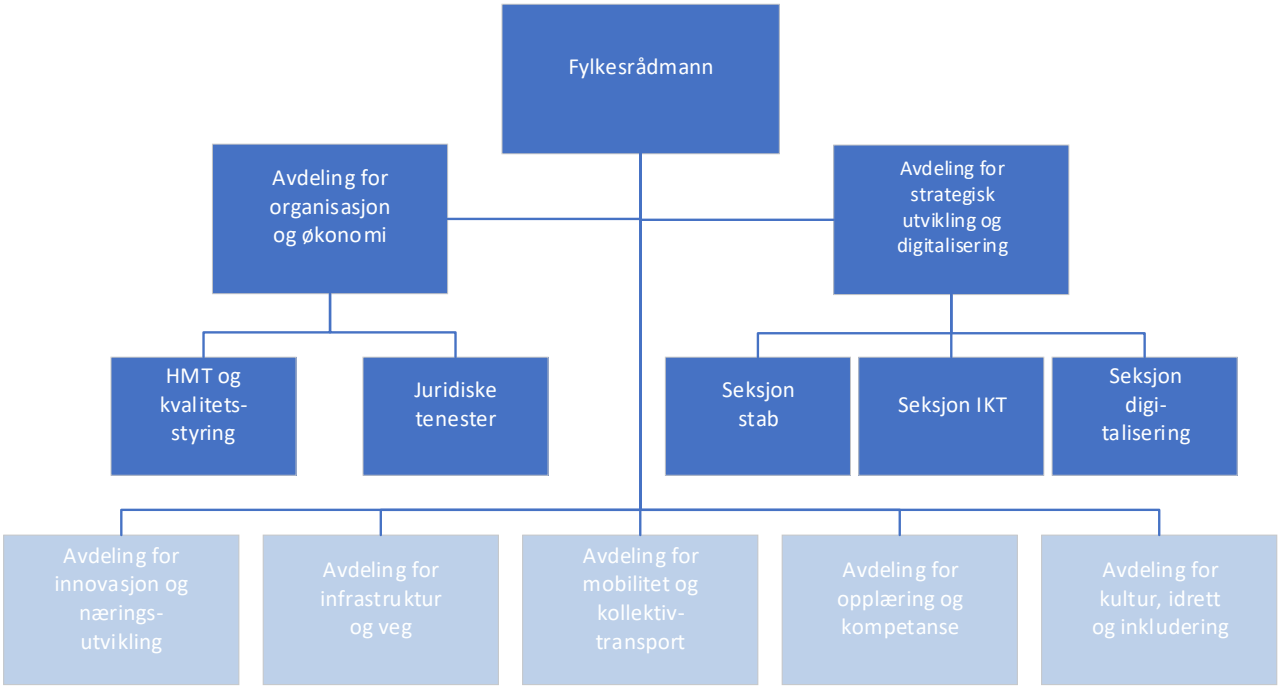
2.2 Organisering, rollar og ansvar

Arbeidet med informasjonstryggleik i Vestland fylkeskommune er fordelt i ulike delar av administrasjonen. Fylkesrådmannen har det overordna ansvaret for at Vestland fylkeskommune sine verdiar blir forvalta på ein effektiv og trygg måte og i samsvar med gjeldande lover, forskrifter og avtalar. Dette inkluderer òg eit overordna ansvar for informasjonstryggleik og personvern. I samband med etableringa av Vestland fylkeskommune blei det bestemt at det var formålstenleg å skilje dei ulike rollene og oppgåvene knytt til informasjonstryggleik også organisatorisk. Sjølve IKT-arbeidet, som systemdrift, kjernedrift, service og tenesteleveranse er einingar under seksjon for IKT i avdeling for strategisk utvikling og digitalisering, medan digitaliserings- og utviklingsarbeidet er skilt ut i ein eigen seksjon for digitalisering i same avdeling. Arbeidet med styringssystemet for informasjonstryggleik er lagt til seksjon stab same avdeling, der ein dedikert ressurs (IKT-sikkerheitsrådgjevar) har som oppgåve å ferdigstille det påbegynte arbeidet med styringssystemet for informasjonstryggleik i Vestland fylkeskommune. Personvernombodet, som arbeider med GDPR og det juridiske knytt til personvern, er plassert i seksjon for juridiske tenester i avdeling for organisasjon og økonomi.

[2] Informasjonsskriv til Deloitte. Vestland fylkeskommune. *Forvaltningsrevisjon informasjonstryggleik Vestland fylkeskommune*. Dato: 09.06.2020.
[3] Information Security Management System
[4] Kvalitetssystemet er levert av Netpower.

Ansvarsfordelinga for informasjonstryggleik i Vestland fylkeskommune går fram i figuren under. I figuren er dei involverte avdelingane utheva, og berre dei underliggande seksjonane som har ei rolle knytt til informasjonstryggleik er vist.[5]

Figur 1: Organisering av informasjonstryggleik i Vestland fylkeskommune



- **Avdeling for strategisk utvikling og digitalisering** har mellom anna ansvar for å samordne den interne aktiviteten i fylkeskommunen gjennom sektorovergripande prosessar, utstrekt bruk av prosjektarbeidsforma og samhandling på tvers av organisasjonseiningar. Avdelinga skal også ta ei leiande rolle i arbeidet med digitalisering.
    - **Seksjon IKT** har ansvar for lokal drift av dei fleste IKT-systema i fylkeskommunen, samt infrastruktur som knyter saman alle lokasjonar. Det er i dag omlag 150 ulike IKT-system i organisasjonen.[6] Seksjonen er frå 1. januar 2020 delt i fire faggrupper (service, tenesteleveranse, systemdrift og kjernedrift).
    - **Seksjon digitalisering** skal sørge for at fylkeskommunen jobbar med digitalisering på ein einsarta, koordinert og strategisk måte. Avdelinga arbeider med fornying, forenkling og effektivisering av prosessar.
    - **Seksjon stab** har mellom anna ansvar for å legge til rette for kommunikasjon og samhandling internt og eksternt, for beredskap og for IKT-tryggleik. Ein rådgjevar for IKT-tryggleik blei tilsett i denne seksjonen i 100 % stilling i april 2020. Vedkommande har sidan tilsettinga arbeidd med å ferdigstille den dokumentasjon som skal gjerast tilgjengeleg for alle tilsette i kvalitetssystemet.

- **Avdeling for organisasjon og økonomi** si hovudoppgåve er drift og utvikling av organisasjonen, samt støttesystema i Vestland fylkeskommune.
    - **Seksjon for juridiske tenester** er organisert direkte under fylkesdirektør for organisasjon og økonomi. I denne seksjonen er det frå 17. august 2020 tilsett **personvernombod** i 50% stilling.
    - **Einings for HMT og kvalitetsstyring** er organisert under HR-seksjonen, men rapporterer direkte til fylkesdirektør og fylkesrådmann. På revisjonstidspunktet er det lyst ut ei stilling som

[5] Opplysningane om avdelinga og seksjonane er henta frå nettsidene til VLFK. Tilgjengeleg frå: https://www.vestlandfylke.no/om-oss/organisasjon/avdeling-for-strategisk-utvikling-og-digitalisering/
[6] Systema som føl med etter overtakinga av Statens vegvesen er ikkje rekna med.

personvernrådgjevar i 100% stilling i denne einninga. Ein medarbeidar i fylkeskommunen fungerer inntil vidare i denne rolla.

I intervju blir det peikt på at denne organiseringa, der dei ulike rollane og oppgåvene ligg til ulike linjer, er formålstenleg mellom anna for å sikre naudsynt uavhengigheit. Det er til dømes viktig at utarbeiding og drift av styringssystemet for informasjonstryggleik ikkje ligg til same eining som dei som skal ivareta den tekniske driftssida (seksjon IKT), og heller ikkje den strategiske digitaliseringssida (seksjon digitalisering). Personvernombodet er lagt til ei eiga gruppa saman med dei andre ombodsfunksjonane for å tryggje den lovpålagte uavhengigheita.

3. Styringssystem for informasjonstryggleik

3.1 Problemstilling

I dette kapittelet vil vi svare på følgjande hovudproblemstilling med underproblemstillingar:

I kva grad har Vestland fylkeskommune etablert styringssystem for informasjonstryggleik som tilfredsstillar krav i sentrale føresegner?

Under dette:

a) Er styrande dokument for informasjonstryggleik i samsvar med krav i regelverket?
b) Er det etablert klåre rutinar og ansvarsforhold knytt til informasjonstryggleik?
c) Har fylkeskommunen system for kontroll og etterprøving av informasjonstryggleik, og blir slik kontroll og etterprøving gjennomført?

3.2 Revisjonskriterium

Artikkel 24 og 28 i forordninga omhandlar den behandlingsansvarlege og databehandlaren sitt ansvar for å etablere internkontroll; nr. 1 i artikkel 24 seier mellom anna at den behandlingsansvarlege skal «gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov», medan artikkel 28 nr. 1 stiller krav om at databehandlarar skal gi tilstrekkeleg med garantiar «for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordningen og vern av den registrertes rettigheter.»

I tillegg til føresegna i personvernforordninga knytt til internkontroll og informasjonstryggleik, er fylkeskommunen gjennom eForvaltningsforskrifta § 15 forplikta til å ha eit internkontrollsystem basert på anerkjende standardar for styringssystem for informasjonstryggleik:

> Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.
>
> Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.

Direktorat for forvaltning og IKT (Difi) er peika ut som ansvarleg for å gje tilrådingar knytt til kva styringssystem for informasjonstryggleik som bør nyttast. Difi tilrår at offentlege verksemder baserer seg på ISO/IEC 27001:2013, som er ein internasjonal standard for styringssystem for informasjonstryggleik. ISO27001:2013 inneheld mellom anna krav om at det skal: fastsettast mål for informasjonstryggleiken i fylkeskommunen, fastsettast overordna policyar (styrande dokument) for informasjonstryggleiken, etablerast eit styringsrammeverk med tydeleg fordeling av rollar, ansvar og oppgåver knytt til informasjonstryggleik i fylkeskommunen, etablerast driftsprosedyrar for informasjonstryggleik, samt at det skal gjennomførast gjennomgang av informasjonstryggleiken.

Sjå vedlegg 2 for utfyllande revisjonskriterium.

3.3 Styrande dokument for informasjonstryggleik

3.3.1 Datagrunnlag

Vestland fylkeskommune er i prosess med å utarbeide eit styringssystem for informasjonstryggleik. Som nemnd i kapittel 2, har dette arbeidet blitt påbegynt fleire gonger, men var på revisjonstidspunktet framleis ikkje ferdig. Fleire av dei sentrale, styrande dokumenta i styringssystemet er likevel ferdige og godkjente. Nokre av desse blei ferdige og godkjente i løpet av revisjonsperioden. Dei styrande dokumenta som er

ferdige og godkjente, er gjort tilgjengelege for dei tilsette i fylkeskommunen gjennom kvalitetssystemet.[7] Kvalitetssystemet blei implementert ved etableringa av den nye fylkeskommunen.

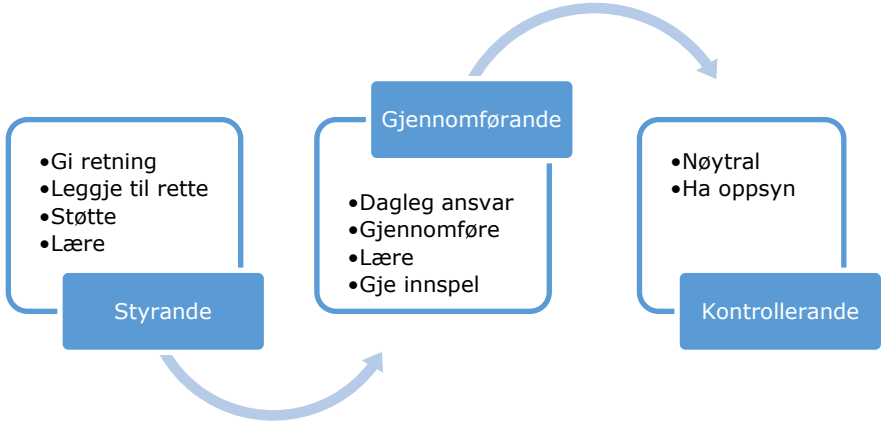
Særleg sentrale blant dei gjeldande, styrande dokumenta i fylkeskommunen sitt styringssystem for informasjonstryggleik er dokumenta *Informasjonssikkerheit og personvern i Vestland fylkeskommune*, *Organisering av informasjonstryggleik* og *Etterleving av informasjonssikkerheit i VLFK*.

Dokumentet *Informasjonssikkerheit og personvern i Vestland fylkeskommune*[8] er det overordna styringsdokumentet i fylkeskommunen sitt styringssystem for informasjonstryggleik. Dokumentet inneheld overordna formål, mål og strategiar for informasjonstryggleik i Vestland fylkeskommune. Det går mellom anna fram at fylkeskommunen har som prioritert målsetting å ivareta informasjonsverdiar på ein forsvarleg og tillitsfull måte, og at fylkeskommunen «uavlateleg» skal arbeide for å oppfylle lovpålagde krav og pliktar knytt til dette. Informasjonstryggleik og personvern er vidare definert verksemdkritiske prosessar i dokumentet.

Vidare i dokumentet er mål og strategiar for informasjonstryggleik punktvis presentert. Til dømes er det eit mål at Vestland fylkeskommune ha høg grad av informasjonstryggleik og personvern. Vidare går det fram at det skal etablerast kontrollar for å beskytte fylkeskommunen sin informasjon og informasjonssystem, at arbeidet med informasjonstryggleik skal integrerast i fylkeskommunen sin daglege drift, at metodane i ISO27001:2013 skal etterlevast, og at det skal etablerast eit system for intern kvalitetssikring på området.

Dokumentet *Organisering av informasjonstryggleik* har som formål å spesifisere rammevilkår og avgrensingar for etablering, implementering, drift og overvaking, gjennomgang, vedlikehald og forbetring av eit dokumentert styringssystem for informasjonstryggleik (ISMS) for Vestland fylkeskommune. Dokumentet skildrar mellom anna organiseringa av informasjonstryggleiksarbeidet i fylkeskommunen, inkludert rollar og ansvarsområde, dei ulike delane i styringssystemet for informasjonstryggleik, samt oppbygginga av sjølve styringssystemet. Rollar og ansvar er skildra i seksjonane 2.2 og 3.4 under. Delane i styringssystemet slik det går fram i dokumentet er presentert i figur 1, og følgjer ein tradisjonell inndeling i *styrande*, *gjennomførande* og *kontrollerande* delar:

Figur 2: Overordna element i styringssystemet for informasjonstryggleik



I dokumentet *Organisering av informasjonstryggleik* går vidare oppbygginga av styringssystemet fram. Styringssystemet til Vestland fylkeskommune er delt inn i tre dokumentnivå, der første nivå omhandlar *kvifor* ein skal ha informasjonstrygglei, andre tar for seg *kva* som må gjerast for å ha informasjonstryggleik, og det tredje forklarar *korleis* dette skal gjerast:

- Dokumenta på ***nivå 1*** er styrande dokument knytt til informasjonstryggleik som samla skal gje ein oversikt over *kvifor* dette arbeidet er viktig. Det overordna styringsdokumentet *Informasjonssikkerheit*

[7] Kvalitetssystemet heiter *Netpower Kvalitet* (sjå https://www.netpower.no/netpower-kvalitet/).
[8] Vestland fylkeskommune. *Informasjonssikkerheit og personvern i Vestland fylkeskommune*. Datert 19.06.2020.

og personvern i Vestland fylkeskommune definerer mål, formål, ansvar og overordna krav.[9] Dette er understøtta av tilleggsdokumenta *Organisering av informasjonstryggleiksarbeidet,*[10] *Risikostyring av informasjonstryggleik*[11] og *Etterleving av informasjonstryggleik.*[12] Dei fleste dokumenta på dette nivået var ferdige, godkjente og gjort tilgjengelege for dei tilsette på revisjonstidspunktet.

- Dokumenta på ***nivå 2*** skal seie *kva* som må gjerast for å etterleve etablert informasjonstryggleiks-policy. Dette er også styrande dokument. På dette nivået er dokumenta *Personelltryggleik innan informasjonstryggleik*, *Sikring av data, Drift og vedlikehald av informasjonssystem, Leverandør-handtering* og *Kontinuitetsplanlegging og handsaming av informasjonstryggleikhendingar*. Dokumenta på dette nivået var på revisjonstidspunktet i varierande grad ferdige, godkjente og tilgjengelege for dei tilsette.

- Dokumenta på ***nivå 3*** er standarar og prosedyrar for informasjonstryggleik, og skal innehalde detaljerte prosedyrar for *korleis* retningslinjene og prinsippa (nivå 2) skal implementerast. Dette er gjennomførande og kontrollerande dokumentasjon. Dokumenta på dette nivået er i liten grad ferdige på revisjonstidspunktet (sjå seksjon 3.4 og 3.5).

Det styrande dokumentet *Etterleving av informasjonssikkerheit i VLFK* inngår på nivå 1 i styringssystemet for informasjonstryggleik i Vestland fylkeskommune. Dokumentet er organisert rundt ein styringsmodell for kontinuerleg forbetring av informasjonstryggleiken i Vestland fylkeskommune. Styringsmodellen er delt inn i fem fasar; planlegging, risikovurdering, tiltak, oppfølging og kontroll, samt rapportering. Styringshjul er presentert i figur 3 under:

Figur 3: Styringshjul for informasjonstryggleik i Vestland fylkeskommune

I dokumentet *Etterleving av informasjonssikkerheit i VLFK* går det fram kva som er formålet med dei ulike fasane, samt kva spørsmål ein skal stille seg for å følgje styringshjulet og slik sikre kontinuerleg forbetring på området. Innhaldet i fasane er kort skildra under:

Fase 1 er *planlegging.* Denne fasa dreier seg om kva eksterne krav til tryggleiken som er gjeldande for Vestland fylkeskommune, kva som er status for tryggleiken i organisasjonen og organisasjonen sine målsetningar innan informasjonstryggleik. Måla skal formulerast i samsvar med S.M.A.R.T.-metodikken; dei skal vere **s**pesifikke, **m**ålbare, **a**nerkjente, **r**ealistiske, **t**idsbestemte og **e**valuerbare.

[9] I *Organisering av informasjonstryggleik* blir det vist til dokumentet *Policy for informasjonstryggleik* og ikkje *Informasjonssikkerheit i Vestland fylkeskommune*. Førstnemnde har revisjonen fått tilsendt i utkastsversjon, der det går frem at dokumentet opphaveleg var utarbeidd for Sogn og Fjordane fylkeskommune.
[10] Vestland fylkeskommune. *Organisering av informasjonssikkerheitsarbeidet*. Datert 29.06.2020.
[11] Dette dokumentet var framleis under utarbeiding på revisjonstidspunktet.
[12] Vestland fylkeskommune. *Etterleving av informasjonssikkerheit.* Datert 09.07.2020.

Fase 2 er *risikovurdering*. Her ser ein på kva som er organisasjonen sine mest kritiske verdiar og kva som er dei største truslane mot desse verdiane. I denne fasen skal det òg definerast kva risikotoleranse organisasjonen har.

Fase 3 er *tiltak*. I denne fasen ser ein på korleis ein skal identifisere, prioritere, bestemme og implementere forebyggande tiltak. I denne fasen skal det òg vurderast om tiltak har ønska effekt.

I **fase 4** tek ein føre seg *oppfølging og kontroll.* Her har ein fokus mellom anna på kva som er gjenstand for revisjon, korleis følgje opp avvik/intern avviksrapportering og korleis følgje opp tryggleiksarbeidet hos tenesteleverandørar. Fasen inneber òg måling av sikkerheit og øvingar innan sikkerheit.

Den siste fasen, **fase 5**, er *rapportering.* I denne fasen skal ein mellom anna sikre kontinuerleg rapportering og sikre at resultatet frå evalueringa dannar grunnlag for nye mål innan førebyggande tryggleik.

Sjølv om dei sentrale, styrande dokumenta som er skildra over er ferdige, godkjende, og gjort tilgjengeleg for dei tilsette gjennom kvalitetssystemet, blir det i intervju sagt at fylkeskommunen framleis har ein veg å gå før også denne delen av styringssystemet er implementert i organisasjonen. Det blir mellom anna vist til at kvalitetssystemet der styringssystemet og desse styrande dokumenta er tilgjengelege, ikkje er gjort tilstrekkeleg kjend i organisasjonen. Som ein følgje av det, blir det antatt i intervju at heller ikkje dei dokumenta i styringssystemet som er ferdige og godkjente, er tilstrekkeleg kjende i organisasjonen. I fleire intervju blir det vidare antatt at dette kan ha negative konsekvensar for etterlevinga av desse styrande dokumenta.

Revisjonen får opplyst er ikkje sett ein endeleg frist for når styringssystemet for informasjonstryggleik i VLFL skal være ferdig. I intervju blir det anslått at dei styrande dokumenta vil vere ferdig utarbeidd i løpet av 2020, og at styringssystemet som heilheit truleg vil vere ferdig implementert i organisasjonen ved utgangen av 2021.

3.3.2 Vurdering

Vestland fylkeskommune er i ferd med å utarbeide sitt styringssystem for informasjonstryggleik. Dei styrande dokumenta i styringssystemet er i hovudsak ferdige og tilgjengelege for dei tilsette. Basert på funna frå undersøkinga har ikkje revisjonen indikasjonar som tyder på at dei ferdige styrande dokumenta bryt med krava i gjeldande regelverk og aktuelle og relevante standardar.

Revisjonen er merksam på at dei styrande dokumenta i styringssystemet for informasjonstryggleik blei godkjende relativt nyleg, og at arbeidet med å implementere styringssystem i fylkeskommunen framleis var pågåande på revisjonstidspunktet. Vidare registrerer vi at både samanslåingsprosessen og COVID-19--pandemien blir vist til som forklaringar for kvifor styringssystemet ikkje er ferdig og ikkje er implementert i organisasjonen. Likevel vil revisjonen understreke viktigheita av å ferdigstille og implementere dei styrande dokumenta for informasjonstryggleik, då dette er ein føresetnad for at leiarar og tilsette i heile organisasjonen veit kva mål og strategi fylkeskommunen har for informasjonstryggleik, og vidare for at fylkeskommunen kan etablere ein god informasjonstryggleikspraksis.

3.4 Rutinar og ansvarsforhold knytt til informasjonstryggleik

3.4.1 Datagrunnlag

Ansvarsforhold for informasjonstryggleik

Styringssystemet for informasjonstryggleik i Vestland fylkeskommune inneheld styrande dokument som skildrar rollar og ansvarsforhold på området. Særleg sentralt er dokumentet *Organisering av informasjons-sikkerheitsarbeidet*. Der går det mellom anna fram at fylkesrådmann har det overordna ansvaret for at Vestland fylkeskommune sine verdiar blir forvalta på ein effektiv og trygg måte i samsvar med gjeldande lover, forskrifter og avtalar. Vidare går det fram kva tilsettekategoriar (rollar) i fylkeskommunen som har kva ansvar, frå fylkesdirektørane via linjeleiarar til seksjonssjefar og tilsette. Kva rolle som har kva ansvarsoppgåver knytt til informasjonstryggleik i Vestland fylkeskommune er kortfatta skildra i tabell 2 under:[13]

Tabell 2: Rolle- og ansvarsdeling knytt til informasjonstryggleik i Vestland fylkeskommune

Rolle	Ansvar
Fylkesrådmann	Har det overordna ansvaret for informasjonstryggleiken i heile verksemda og ansvar for:

[13] I tillegg til rollene i tabellen, blir også ansvaret til vakt og sikring og bygg og eigedom skildra i dokumentet.

(styrande funksjon)	• Forankring av arbeidet med informasjonstryggleik i toppleiargruppa • Gjennomføring av årleg gjennomgang av informasjonstryggleiksarbeidet i leiargruppa • Avsette nødvendige ressursar for å ivareta tryggleiken i organisasjonen • Ha ei klar forståing av kva verdiar organisasjonen forvaltar og truslar mot desse • Skille kontrollerande og utøvande oppgåver
Fylkesdirektørar	Har det dagleg operative ansvaret for informasjonstryggleik og ansvar for å: • Sikre at linjeorganisasjonen utfører sine oppgåver • Syte for jamlege oppfølging av mål og strategiar for informasjonstryggleik • Gjennomføre ein årleg eigenkontroll og sikre at tiltaka etter denne blir fylgt opp • Støtta fylkesrådmannen i verdivurdering og andre årlege evalueringar
Linjeleiarar	Har ansvar for at tryggleiksarbeidet blir utøvd og kontrollert ut frå fastsette krav og rutinar og har såleis ansvaret for å praktisere arbeidet med informasjonstryggleik og å gjennomføre internkontroll, samt ansvar for å: • Tryggleiken innan eige ansvars- og myndigheitområde, inkludert der utføringa av tryggleiksoppgåver er tenesteutsett til private leverandørar eller andre organisasjonar • Sørge for at eige personell har gjennomgått grunnleggande opplæring i tryggleik • Å rettleie sine medarbeidarar og sjå til at dei tenkjer tryggleik inn i arbeidet • Å handtere situasjonar dersom medarbeidarane ikkje ser ut til å ivareta tryggleiken på ein tilfredsstillande måte • Ha oversikt over den tryggleiksfaglege kompetansen i organisasjonen generelt, og ha rutinar som sikrar at kompetanse utviklast og blir vedlikehalde
IKT-sikkerheits-rådgjevar (utøvande funksjon)	Har oppgåver som inneberer koordinering, rådgjeving og kontroll av IKT- tryggleiksarbeidet i organisasjonen, og har det faglege og praktiske ansvaret for utvikling og vedlikehald av styringssystemet for informasjonstryggleik. IKT-sikkerheitsrådgjevar skal: • Jobbe sektorovergripande saman med rådgjevar for beredskap, og inn mot seksjonane for IKT og digitalisering • Rådgje i IKT-tryggleiksspørsmål i linje og prosjekt • Gjennomføre og følgje opp tekniske ROS-vurderingar • Planlegge og gjennomføre aktivitetar knytt til informasjonstryggleiksområdet derunder bidra til å bygge ein god tryggleikskultur • Fortløpande vurdere potensielle sårbarheiter og rapportere til leiinga • Bidra i handtering av uønskte hendingar og fasilitere IT-beredskapsøvingar • Delta i utvikling av nye løysingar og kontinuerleg forbetring av eksisterande løysingar • Sørge for at dokumentasjon er på riktig nivå og oppdatert • Ansvar for implementering og vedlikehald av styringssystem for informasjonstryggleik. • Fortløpande kontrollere at tryggleikstiltak som er pålagt eller vedtatt etablert faktisk er iverksett og fungerer etter sin hensikt • Motivering og bevisstgjering om behovet for førebyggande tryggleik Stillinga har fullmakt til mellom anna å kunne foreslå og gjennomføre opplæring i informasjonstryggleik, risikovurderingar, tryggleikstestar, avvikshandsaming, og iverksette korrigerande og andre tryggleiksrelaterte tiltak som er vedtekne.
Seksjonssjef/rektorar	Har ansvar for at fylkeskommunen sine mål og strategiar for informasjonstryggleik blir følgd opp i eigen seksjon/eining/skule og at det blir drive systematisk og kontinuerleg arbeid med personvern. Oppgåvene inkluderer: • Ansvar for å forankre personstryggleiksarbeidet i eiga leiargruppe og blant dei tilsette i/på seksjonen/eininga/skulen • Sikre at eininga sitt arbeid med informasjonstryggleik er organisert hensiktsmessig etter retningslinjene frå styrande dokument.
Systemeigar	• Systemeigar har ansvar for heile livssyklusen til eit informasjonssystem. • Systemeigar har det overordna ansvaret for at rollane hos fagavdelinga er ivaretatt og avtalar inngått. I det ligg det også at det er avsett tilstrekkeleg med ressursar. Alle system og alle typar informasjon skal ha ein definert eigar • Systemeigaren skal definere kva for brukarar eller brukargruppe som skal ha tilgang til informasjon og kva som er autorisert bruk av informasjonen. Systemeigar er bestillar/funksjonell premissgivar innan systemet sitt funksjonsområde. Det skal vere eintydig kven som har rolla som systemeigar for eit system.
Alle tilsette[14]	• Har ansvar for det daglege tryggleiksarbeidet • Være bevisste på tryggleik i kvardagen

[14] Det går òg fram i styringsdokumentet at også innleigd personell må følgje tryggleikskrava på lik linje med organisasjonen sine eigne tilsette, samt at slike innleigde ressursar må tydeleg informerast om gjelande reglar i fylkeskommunen.

- Følgje instruksar for den praktiske gjennomføring av tryggleik i verksemda
- Kjenne til tryggleiksorganisasjonen i verksemda
- Kjenne til prinsippa for risikostyring
- Påpeike feil og manglar ved tryggleiken i verksemda

I fleire intervju blir det opplyst at det den formelle fordelinga av rollar og ansvar knytt til informasjonstryggleik berre delvis blir praktisert som forutsett. Dette blir i hovudsak tilskrive at styringssystemet for informasjonstryggleik framleis er under utarbeiding, og at fleire tilsette på ulike nivå i organisasjonen difor ikkje er tilstrekkeleg kjende med kva ansvar dei har når det gjeld informasjonstryggleik. Som døme på dette blir det peika på at ikkje alle systemeigarar er klar over at dei innehar denne rolla, eller kva oppgåver som ligg til rolla.

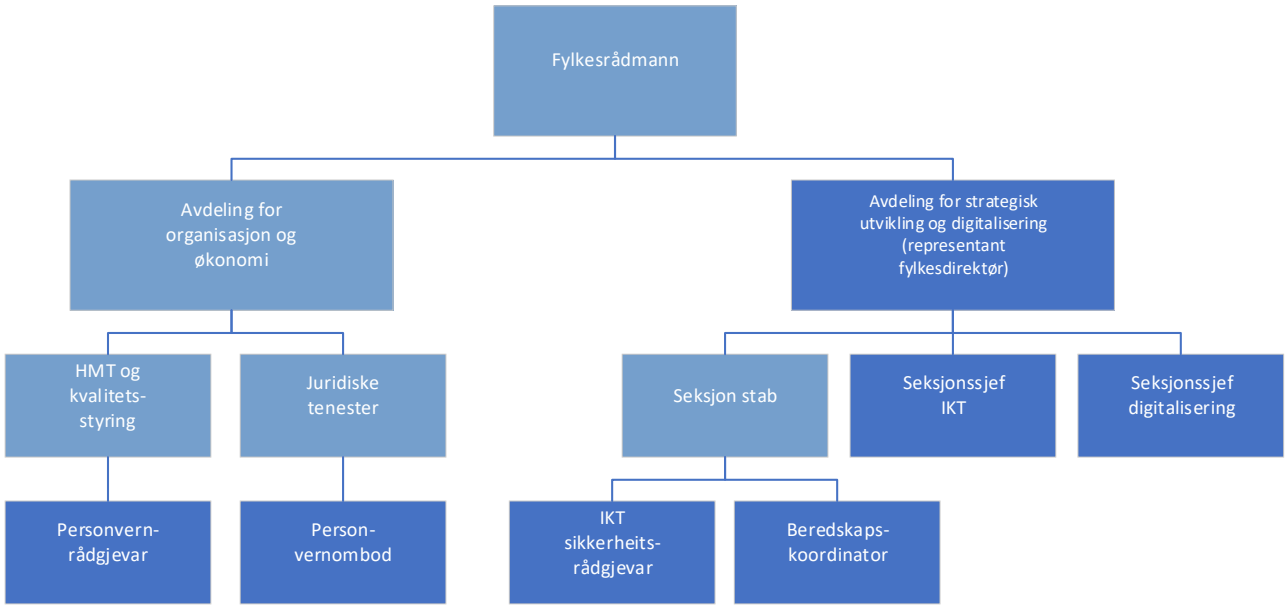
Dette er understøtta i resultata frå spørjeundersøkinga. Av dei 21 respondentane som svarte at dei var anten systemeigar eller systemforvaltar for eit eller fleire fagsystem i fylkeskommunen, svarte om lag 15 % at dei anten «i liten grad» (9,5 %) eller «i svært liten grad» (4,8 %) opplever at det er tydeleg kva informasjonstryggleiksansvar som følgjer med å vere systemeigar/ systemforvaltar.[15] På leiarnivå var svara noko annleis; av dei 62 respondentane som svarte at dei er leiarar i fylkeskommunen, svarte dei fleste at dette informasjonstryggleiksansvaret som låg til rolla er tydeleg, medan ca. 22 % svarte at det «i verken stor eller liten grad» er tydeleg.[16] Blant dei tilsette svarte også dei fleste at dei var kjende med kva informasjonstryggleiksansvar som ligg til deira stilling; likevel svarte over éin av fire (26 %) at dei «i verken stor eller liten grad» var kjende med dette ansvaret, og éin av tolv (ca. 8 %) svarte at dei «i liten grad» var kjende med dette.[17]

I intervju blei det også peika på at ansvaret som ligg til toppleiarane i Vestland fylkeskommune knytt til informasjonstryggleik i varierande grad blir ivaretatt. Det blei mellom anna kommentert at arbeidet med informasjonstryggleik ikkje er gjennomgåande forankra i toppleiinga i Vestland fylkeskommune. Det blir vist til at dette kan skuldast at ein ikkje har kome langt nok i prosessen med å etablere retningslinjer og rutinar for dette arbeidet i fylkeskommunen. I intervju blir det likevel understreka at alle fylkesdirektørane må engasjere seg i informasjonstryggleiksarbeidet i eiga avdeling for å kunne bygge ein tilstrekkeleg kultur for arbeid med informasjonstryggleik. Det blir òg vist til at manglande forankring i toppleiinga kan føre til manglande forankring på leiarnivåa som er organisert under fylkesdirektørnivået, som igjen kan føre til manglande informasjonstryggleikskultur på nivåa under. I spørjeundersøkinga svarte om lag 12 % at det anten «i liten grad» (10,7%) og «i svært liten grad» (1,2%) er tilstrekkeleg fokus på informasjonstryggleik i fylkeskommunen.[18]

Fylkeskommunen har òg etablert eit sikkerheitsforum for informasjonstryggleik og personvern. Sikkerheitsforum skal understøtte fylkeskommunen sitt arbeid med informasjonstryggleik og personvern. Som det går fram av figur 4 under, består sikkerheitsforum av representant for fylkesdirektør for strategisk utvikling og digitalisering, Seksjonssjef IKT, Seksjonssjef digitalisering, IKT sikkerheitsrådgjevar, Personvernrådgjevar, Personvernombod og Beredskapskoordinator. Sikkerheitsforumet skal møtast seks gonger i året, og skal forankre god informasjonstryggleik og personvern i Vestland fylkeskommune, samt vere eit knytepunkt for samhandling mellom dei sentrale avdelingane som er involvert i det overordna arbeidet med informasjonstryggleik og personvern (avdeling for organisasjon og økonomi og avdeling for strategisk utvikling og digitalisering). I korrespondanse med fylkeskommunen får revisjonen opplyst at sikkerheitsforumet formelt er etablert, men at det ikkje har vore aktivitet i gruppa enno. Etter planen skal første møte vere før jul 2020.

[15] 23,8 % svara «i svært stor grad», 28,6 % svara «i stor grad», 33,3 % «i verken stor eller liten grad», 9,5 % svara «i liten grad» og 4,8 % svara «i svært liten grad».
[16] N=62. 22,6 % svara «i svært stor grad», 51,6 % svara «i stor grad», 3,2 % svara «i liten grad» og 0,0 % svara «i svært liten grad».
[17] N=322. 17,4 % svara «i svært stor grad», 46,3 % «i stor grad», og 1,6 % «i svært liten grad».
[18] N=327. 8,0 % svarar «i svært stor grad», 40,4 % svara «i stor grad», 39,8 % svara «i verken stor eller liten grad».

Figur 4: Sikkerheitsforum, Vestland fylkeskommune



Rutinar for informasjonstryggleik

Som nemnd er styringssystemet for informasjonstryggleik i Vestland fylkeskommune framleis under utarbeiding, og det er særleg dokumenta på nivå 2 og 3 som manglar. Nokre av dokumenta på desse nivåa er likevel ferdige, godkjende og tilgjengelege for dei tilsette i kvalitetssystemet.

På nivå 2, er særleg *Handbok for informasjonssikkerheit og personvern for Vestland fylkeskommune* sentralt.[19] Dokumentet er det sentrale informasjonstryggleiksreglementet som skal etterlevast av alle tilsette i Vestland fylkeskommune. Dokumentet omhandlar mellom anna heimel og prinsipp for behandling av personopplysningar, grunnsikring av infrastruktur og tenester, internkontroll, avvik (sjå seksjon 6.7), databehandlaravtalar, og systemtryggleik.

Andre dokument på nivå 2 i styringssystemet som er ferdige, godkjende og tilgjengelege er:

- *Clean Desk Policy.*[20] Dette dokumentet skildrar korleis tilsette skal forlate arbeidsplassen og at tilsette alltid skal sørge for at det ikkje ligg sensitiv, konfidensiell eller beskytta dokument eller anna informasjon tilgjengeleg på pulten eller arbeidsplassen når ein forlèt den.
- *IT-sikkerheitsreglar for tilsette og eksterne i Vestland fylkeskommune*.[21] Retningslinjene er basert på ISO27001 og blir nærare skildra i seksjon 7.3.
- *Retningslinjer for leverandørstyring og IT-anskaffingar*.[22] Dette dokumentet skildrar informasjons-tryggleikspolicyen for relasjonar til leverandørar av IT-system. Vidare er det utarbeida ei sjekkliste som mellom anna etterspør om det er gjennomført ROS-vurdering, PIA/DPIA-vurdering (sjå seksjon 6.6) og om det er støtte for AD-integrasjon for tilgjengestyring (sjå seksjon 5.3).

På nivå 3 i styringssystemet er følgjande dokument godkjente og tilgjengelege i kvalitetssystemet:

- *Informasjonssikkerheit og personvern til innkjøp v. utlysing av anbod*.[23] Her går det fram at leverandøren skal gjennomføre eigne tekniske og organisatoriske tiltak for å sikra at all behandling i samband med gjennomføring av leveransen oppfyller krava i Personvernlovgjevinga.
- *Passord policy Vestland fylkeskommune*.[24] Dette dokumentet skildrar kva reglar og retningslinjer som gjeld for brukarpassord i Vestland fylkeskommune for alle som har ein brukarkonto i minst eitt av IT-

[19] Vestland fylkeskommune. *Handbok for informasjonssikkerheit og personvern for Vestland fylkeskommune*. 22.09.2020.
[20] Vestland fylkeskommune. *Clean desk policy*. Datert 04.09.2020
[21] Vestland fylkeskommune. *It-sikkerheitsreglar for tilsette og eksterne for Vestland fylkeskommune.* 07.10.2020.
[22] Vestland fylkeskommune. *Retningslinjer for leverandørstyring og IT-anskaffingar*. 10.08.2020
[23] Vestland fylkeskommune. *Informasjonssikkerheit og personvern til innkjøp v. utlysing av anbod.* 17.06.2020
[24] Vestland fylkeskommune. *Passord policy Vestland fylkeskommune.* 10.08.2020

systema eigd av Vestland fylkeskommune. Det vil seie alle tilsette, lærlingar og innleigde eksterne konsulentar.

I intervju får revisjonen opplyst at resten av dokumenta som vil inngå i nivå 2 og nivå 3 i styringssystemet framleis er under utarbeiding og at desse skal ferdigstillast saman med systemeigarar og brukarar. Det blir understreka at ein ikkje kan ferdigstille arbeidet med dokumenta på nivå 3, før dokumenta på nivå 1 og nivå 2 er klare.

Andre rutinar

Revisjonen har òg fått tilsendt ei rekkje retningslinjer og rutinar knytt spesifikt til personvern. Desse inngår ikkje i styringssystemet for informasjonstryggleik, men er anten tilgjengeleg i kvalitetssystemet i mappa «Personopplysningar», eller under mappa «Personvern og informasjonstryggleik».

Dokumenta i mappa «Personopplysningar» inkluderer *Retningslinjer for innhenting og tilbaketrekking av samtykke*,[25] *Retningslinjer for kva for og korleis informasjonen skal gjevast til den registrerte ved innhenting av personononopplysningar*,[26] og *Retningslinjer og rutinar for sletting.*[27]

Retningslinjer for innhenting og tilbaketrekking av samtykke skildrar når samtykke skal innhentast, korleis samtykke skal innhentast, kva krav som stillast til samtykke, korleis fylkeskommunen skal dokumentere at den registrerte har gitt samtykke og korleis den registrerte skal kunne trekke tilbake eit gitt samtykke. *Retningslinjene for kva for og korleis informasjonen skal gjevast til den registrerte ved innhenting av personopplysningar* slår fast at den registrerte har rett til å få informasjon om at fylkeskommunen behandlar personopplysningar til vedkommande, til kva formål, korleis og kor lenge personopplysningane behandlast. *Retningslinjer og rutinar for sletting* skildrar kva som skal slettast, når fylkeskommunen har ei sjølvstendig plikt til å slette personopplysningane og kva tid til fylkeskommunen kan unnlata å slette personopplysningar.

I mappa «Personvern og informasjonstryggleik» ligg ei rekkje malar og retningslinjer, mellom anna knytt til databehandlaravtalar, samtykke, samt behandling av persopplysningar meir generelt. Dei fleste dokumenta er framleis under utarbeiding, og er verken godkjende eller gjort tilgjengelege for dei tilsette.

Dette gjeld mellom anna utkast til rutinedokumentet *Rutine for ny behandling av personopplysningar.*[28] Formålet med rutinen er å sikra og dokumentere at fylkeskommunen sine nye behandlingar av person-opplysningar oppfyller krava i personvernforordninga. Dokumentet inneheld mellom anna ei sjekkliste som skal fyllast ut før fylkeskommunen iverksett ny behandling av personopplysningar. Sjekklista skal lagrast i tilknyting til behandlingsprotokollen for den aktuelle eininga/avdelinga i kvalitetssystemet (sjå seksjon 6.4). Det er den som har ansvaret for å iverksette ny behandling skal sikre at sjekklista blir fylt ut. I sjekklista må den ansvarlege mellom anna vurdere om fylkeskommunen er databehandlar for behandlinga (sjå seksjon 6.4), om det er naudsynt å gjennomføre ein DPIA (sjå seksjon/avsnitt 6.6), og kva kategori av personopplysningar som blir behandla. Rutinen skal gjennomgåast og godkjennast av avdelinga/einings sin personvernkoordinator, ved behov etter dialog og rådgjeving frå personvernombodet (sjå seksjon 6.3).

I korrespondanse med fylkeskommunen får revisjonen opplyst at nokre av dokumenta som ligg i kvalitetssystemet er utdaterte og ikkje lenger i bruk, og at andre er plassert feil. Det er planlagt eit oppryddingsarbeid for å sikre at det er eintydig kva rutinar som er gjeldande.

3.4.2 Vurdering

Undersøkinga viser at delane av styringssystemet for informasjonstryggleik som so langt er ferdig og tilgjengeleg for tilsette i kvalitetssystemet mellom anna skildrar kva ansvarsforhold og roller som er knytt til arbeidet med informasjonstryggleik. Informasjon både frå intervju og spørjeundersøking tyder på at dei formelle rollane ikkje blir praktisert som føresett; t.d. er ikkje alle med systemeigaransvaret klar over at dei har denne rolla. Undersøkinga avdekker vidare at arbeidet med informasjonstryggleik ikkje i tilstrekkeleg grad er forankra på toppnivå i organisasjonen.

[25] Vestland fylkeskommune. *Retningslinjer for innhenting og tilbaketrekking av samtykke.* 09.07.2020.
[26] Vestland fylkeskommune. *Retningslinjer for kva for og korleis informasjon skal gjevast til den registrerte ved innhenting av personopplysningar [SIC]*. 09.07.2020.
[27] Vestland fylkeskommune. *Retningslinjer og rutinar for sletting.* 09.07.2020.
[28] Vestland fylkeskommune. *Rutine for behandling av personopplysningar.* Ikkje datert.

Revisjonen er merksam på at rollar og ansvar på området relativt nyleg er formalisert. Likevel vil vi understreke at manglande etterleving av den formelle rolle- og ansvarsdelinga knytt til informasjonstryggleik aukar risikoen for brot på regelverk, svak informasjonstryggleik, og for at det oppstår avvik både knytt til informasjonstryggleik og personvern. Som følgje av at fylkeskommunen har arbeidd med styringssystemet parallelt med gjennomføringa av denne forvaltningsrevisjonen, kan rollar og ansvar knytt til informasjonstryggleik vere betre kjent og i større grad praktisert i dag enn det funna frå undersøkinga tyder på. Det er likevel revisjonen si vurdering at Vestland fylkeskommune på revisjonstidspunktet ikkje har ein praksis som er i samsvar med ISO27001:2013 punkt 5.3, som seier at ansvar og mynde for rollar som er relevante for informasjonstryggleik skal vere tildelt og kommunisert. Revisjonen meiner at Vestland fylkeskommune i større grad må gjere ansvarsforholda knytt til informasjonstryggleik kjende i organisasjonen.

Vidare viser undersøkinga at det er utarbeidd fleire rutinar og retningslinjer for informasjonstryggleik i fylkeskommunen sitt styringssystem. Fleire av desse – og særleg *Handbok for informasjonssikkerheit og personvern for Vestland fylkeskommune* og *IT-sikkerheitsreglar for tilsette og eksterne i Vestland fylkeskommune* – omhandlar sentrale informasjonstryggleiksprinsipp, og skildrar korleis og kvifor tilsette skal praktisere god informasjonstryggleik. Revisjonen er merksam på at styringssystemet framleis er under utarbeiding, og registrerer at fylkeskommunen er open på at ikkje alle rutinar, prosedyrar og retningslinjer for informasjonstryggleik er ferdige. Samtidig viser undersøkinga at det finst fleire rutinar, prosedyrar og retningslinjer i kvalitetssystemet til fylkeskommunen som omhandlar informasjonstryggleik og personvern, men som *ikkje* inngår i styringssystemet for informasjonstryggleik. Basert på det som kjem fram i korrespondanse med fylkeskommunen, er nokre av desse utdaterte, medan andre er feilplassert i kvalitetssystemet. Ein slik situasjon, der styringssystemet ikkje er ferdig, og det parallelt eksisterer rutinedokument som omhandlar same tema, meiner revisjonen er uheldig. Det er då svært vanskeleg for den enkelte tilsette å vite kor ein finn rutinar og retningslinjer på området, samt kva av desse som faktisk er gjeldande. Dette kan både føre til at tilsette følgjer rutinar som ikkje gjeld og ikkje finn dei rutinane som gjeld. Konsekvensane av ein slik situasjon kan vere at tilsette ikkje praktiserer informasjonstryggleik i samsvar med gjeldande rutinar, med tilhøyrande risiko for brot på både interne rutinar og ekstern regelverk.

3.5 Kontroll og etterprøving av informasjonstryggleik

3.5.1 Datagrunnlag

Vestland fylkeskommune har formelt etablert system og rutinar for kontroll og etterprøving av informasjonstryggleiken i fylkeskommunen. Særleg sentralt er styringsdokumentet *Organisering av informasjonssikkerheitsarbeidet*. Der går det fram at for å sikre at styringssystemet for informasjons-tryggleik fungerer som forutsett og fylkeskommunen si praksis på området er god, er det viktig at fylkesrådmannen minst éin gong i året evaluerer tryggleikstilstanden i verksemda (dette blir gjerne kalla leiinga si gjennomgang).

Evalueringa skal formaliserast som eit møte og må dokumenterast skriftleg. Som del av dokumentasjonen skal det gå fram kva risiko som er akseptert, kva risiko som må handterast, og kva tiltak som skal settast i verk. Den årlege evalueringa skal mellom anna ta utgangspunkt i tilbakemeldingar frå eksterne tilsyn, registrerte avvik, erfaringar frå risikohandtering, læring frå penetrasjonstesting, rapportering på målinnfriing innan tryggleik, endringar i trusselbilete, samt kontroll med tryggleiksarbeidet i underliggande organisasjon.

Det går også fram at fylkeskommunen mellom anna skal gjennomføre penetrasjonstesting og føre kontroll med tryggleiksarbeidet i organisasjonen, og at dette skal leggast til grunn for den årlege evalueringa av tryggleikstilstanden i verksemda.

Det er IKT-seksjonen i samarbeid med IKT-sikkerheitsrådgjevar som skal gjennomføre teknisk kontroll og etterprøving av informasjonssystema, til dømes gjennom sokalla penetrasjonstesting.[29] Vestland fylkes-kommune har rammeavtalar med konsulentselskap som har kompetanse på området, og har dermed moglegheit til å bestille slik testing.[30]

[29] Ein penetrasjonstest er eit autorisert, simulert angrep på eit datasystem, utført for å evaluerer tryggleiken til systemet.
[30] Revisjonen får opplyst at det før etableringa av Vestland fylkeskommune 1. januar 2020 blei gjennomført fullskalatesting av basis infrastruktur i Vestland fylkeskommune, med fokus på driftstryggleik.

I intervju blir det opplyst at det ikkje har blitt gjennomført testar og kontrollar av informasjonstryggleiken i fylkeskommunen slik styringssystemet føresett, og at det heller ikkje har blitt gjennomført interne eller eksterne evalueringar, gjennomgangar eller tilsyn etter etableringa av Vestland fylkeskommune. Heller ikkje den årlege evalueringa av styringssystemet har so langt blir praktisert som føresett.

Det blir også i denne samanheng peika på at styringssystemet ikkje er ferdig, og at organisasjonen framleis har ein veg å gå før både dette er implementert og organisasjonen har ein moden tryggleikskultur. I tillegg går det fram frå i kvalitetssystemet at styringsdokumentet som regulerer denne delen av styringssystemet for informasjonstryggleik (*Organisering av informasjonssikkerheitsarbeidet*) blei godkjent i juni 2020.

3.5.2 Vurdering

Vestland fylkeskommune har etablert system og rutinar for kontroll og etterprøving av informasjonstryggleik, men funna i undersøkinga viser at desse ikkje blir praktisert eller etterlevd som forutsett. Revisjonen registrerer at fylkeskommunen viser til det at styringssystemet ikkje er ferdig som årsak til at kontroll og etterprøving av informasjonstryggleiken enno ikkje har funnet stad. Det er likevel revisjonen si vurdering at fylkeskommunen ikkje oppfyller sentrale krav til i eForvaltningsforskrifta § 15 eller tilrådingar i ISO27001:2013 knytt til oppfølging og kontroll.

4. Konfidensialitet

4.1 Problemstilling

I dette kapittelet vil vi svare på følgjande hovudproblemstilling med underproblemstillingar:

I kva grad har Vestland fylkeskommune etablert rutinar for sikring av konfidensialitet, og i kva grad blir disse etterlevd?

Under dette:

a) Hindre uautorisert innsyn i konfidensielle opplysningar
b) Sikker sone for lagring av konfidensielle opplysningar
c) Kryptering av konfidensielle opplysningar

4.2 Revisjonskriterium

Konfidensialitet er ein av dei grunnleggjande informasjonstryggleiksdimensjonane, saman med *integritet* og *tilgjengelegheit*. Å sørgje for *konfidensialitet* inneber å hindre ikkje-autorisert innsyn i informasjon som ikkje skal vere tilgjengeleg for alle. I ISO27001:2013 inneheld særleg punkta 8.2 *Klassifisering av informasjon*, 8.3 *Håndtering av medier*, 9.2 *Styring av brukeraksess*, og 10 *Kryptografi* viktige retningslinjer for korleis sikre konfidensialitet.

Personvernforordninga artikkel 32 nr. 1 stiller krav om informasjonstryggleik ved behandling av person-opplysningar. Krava som blir stilt er at informasjonstryggleiken skal vere tilfredsstillande med omsyn til personopplysningane si **konfidensialitet**, integritet, tilgjengelegheit og robustheit gjennom at det blir sett i verk eigna tekniske og organisatoriske tiltak basert på risikovurderingar. Artikkelen inneheld føresegn som omhandlar kva risikovurderingane skal leggje vekt på. Tiltak som også blir nemnd under artikkel 32 nr. 1 er pseudonymisering og kryptering av personopplysningar og evne til å rette opp igjen tilgjengelegheita og tilgangen til personopplysningar i rett tid dersom det oppstår ein fysisk eller teknisk hending.

Sjå vedlegg 2 for utfyllande revisjonskriterium.

4.3 Hindre uautorisert innsyn i konfidensielle opplysningar

4.3.1 Datagrunnlag

Rutinar

Vestland fylkeskommune har etablert fleire retningslinjer og rutinar som omhandlar korleis hindre uautorisert innsyn i konfidensielle opplysningar. I det styrande dokumentet *Organisering av informasjons-sikkerheitsarbeidet* (nivå 1) blir det t.d. stilt krav om at alle avtalar som angår IKT-system som er drifta av eksterne leverandørar skal innehalde krav til informasjonstryggleik, inkludert med omsyn til konfidensialitet.

Vidare, i *Handbok for informasjonssikkerheit og personvern for Vestland fylkeskommune* (nivå 2) går det fram at konfidensialitet skal sikre mot ikkje-autorisert innsyn i, endring av eller offentleggjering av informasjon og data. I handboka går det vidare fram at Vestland fylkeskommune «for konsolidert og klassifisert informasjon prioritera omsynet til konfidensialitet føre omsynet til tilgjengelegheit og integritet». Handboka inneheld også ein oversikt over Vestland fylkeskommune sine konfidensialitetsklasser som seier noko om kva konfidensialitetskrav som blir stilt til ulike klasser informasjon (sjå seksjon 4.4).

Som nemnd i seksjon 3.4, har Vestland fylkeskommune også utarbeidd *IT-sikkerheitsreglar for tilsette og eksterne for Vestland fylkeskommune* (nivå 2). I dokumentet går det fram korleis dei tilsette skal stille seg til konfidensialitet, integritet og tilgjenge til informasjonen Vestland fylkeskommune forvaltar, og dei tilsette blir mellom anna pålagt å låse datamaskina si når den ikkje er i bruk, stå ved skrivaren når dokument blir prenta ut, og ta ansvar for at det ikkje blir liggande att papir ved skrivaren. Vidare går det fram i reglementet at tilsette skal vere varsam med å opne e-postar og klikke på lenker der dei er usikre på avsendar og innhald. Om tilsette er i tvil om ein e-post er autentisk, skal dei ringje avsendar. Desse

sikkerheitsreglane blei godkjente i oktober 2020, og det har ikkje blitt gitt opplæring i desse eller innanfor informasjonstryggleiksområdet generelt (sjå kapittel 7).

Vidare har revisjonen har fått tilsendt to ulike skjema der tilsette i Vestland fylkeskommune skal stadfeste at dei har teieplikt. Ein av malane, *Fråsegn om teieplikt*[31] gjeld for tilsette i fylkeskommunen med tilgang til konfidensielle opplysningar. I dokumentet blir det peika på at teieplikta er pålagt ein kvar som utfører tenester eller arbeid for eit forvaltningsorgan etter forvaltningslova § 13. Teieplikta gjeld òg etter at ein tilsett er slutta i arbeidet. Revisjonen har også fått tilsendt skjemaet *Teieplikterklæring*.[32] Her blir går fram at teieplikta gjeld for både for dokument og for munnleg informasjon.

I *Handbok for informasjonssikkerheit og personvern for Vestland fylkeskommune* går det fram at det er HR-direktøren som gjennom tilsetjingsprosessen skal syte for at alle tilsette, samarbeidspartnarar og mellombels tilsette har underteikna teieplikterklæringa.

Praksis

Det blir i intervju peika på auka medvit knytt til konfidensialitet i Vestland fylkeskommune. Sentrale personar innan informasjonstryggleik i organisasjonen fortel at tilsette i større grad tek kontakt med spørsmål knytt til konfidensialitet og personvern. Dette har særleg blitt aktuelt med auka bruk av digitale kommunikasjonsverktøy under COVID-19-pandemien.

Revisjonen får opplyst at det ikkje har blitt gjennomført datainnbrot mot Vestland fylkeskommune eller at det har vore konkrete hendingar som har ført til uautorisert innsyn i konfidensielle opplysningar. I intervju får revisjonen likevel opplyst at tilsette ikkje alltid lev opp til ynskja informasjonstryggleikspraksis; til dømes blir det fortalt om passord på lappar i nærleiken av datamaskina, og at mange tilsette trykkjer på lenkjer i e-postar sjølv om ein i delar av organisasjonen har arbeidd med å informere om at dette fører til dårlegare informasjonstryggleik. Det går også fram i spørjeundersøkinga at fleire tilsette opplever at det blir sendt personopplysningar via mail.

4.3.2 Vurdering

Vestland fylkeskommune har fleire retningslinjer og rutinar som etter revisjonen si vurdering er eigna til å bidra til å hindre uautorisert innsyn i konfidensielle opplysningar. Funn i undersøkinga tyder likevel på at tilsette i ikkje alltid etterlev desse retningslinjene og rutinane. Det er følgjeleg revisjonen si vurdering at fylkeskommunen ikkje i tilstrekkeleg grad hindrar uautorisert innsyn i konfidensielle opplysningar. I den samanheng vil revisjonen særleg peike på viktigheita av at fylkeskommunen sine tryggleiksreglar knytt til e-postbruk blir etterlevd. Sannsynet for at konfidensielle opplysningar kjem på avvege om slike blir sendt per e-post er relativt høg, og konsekvensane kan vere negative både for fylkeskommunen og for dei opplysningane angår. Vidare er det svært viktig at dei tilsette praktiserer trygg e-postbruk når det gjeld vedlegg og lenkar; konsekvensane av at berre éin tilsett trykkar på ein falsk lenke eller opnar eit vondsinna vedlegg kan vere dramatiske for både fylkeskommunen sjølv, og for fylkeskommunen sine tenestemottakarar, då det kan gje vondsinna aktørar tilgang til fylkeskommunen sine system og informasjonen som ligg der.

4.4 Lagring av konfidensielle opplysningar

4.4.1 Datagrunnlag

Korleis lagring av konfidensielle opplysningar skal skje i Vestland fylkeskommune er omtalt i fleire styrande dokument på ulike nivå i fylkeskommunen sitt styringssystem for informasjonstryggleik. I *Organisering av informasjonssikkerheitsarbeidet* (nivå 1) går det t.d. fram at informasjon skal klassifiserast med omsyn til tryggleiksnivå og tilgangsavgrensing, og at det skal gjennomførast risikovurderingar for å klassifisere informasjonen ut frå kor kritisk den er for verksemda. Slik klassifisering er nærare skildra i *Handbok for informasjonstryggleik og personvern i Vestland fylkeskommune* (nivå 2). Der går det frem at informasjon skal klassifiserast i fire konfidensialitetklasser, med tilhøyrande reglar for tilgangsstyring (sjå tabell 3):

[31] Vestland fylkeskommune. *Fråsegn om teieplikt.* Ikkje datert.
[32] Vestland fylkeskommune. *Teieplikterklæring.* Ikkje datert.

Tabell 3: Konfidensialitetsklasser

Klasse	Type data (dømer)	Tilgang	Merknader
Open	Nett-side som presenterer ein avdeling eller eining som blir lagt ope ut på internett	Informasjon kan eller skal vere tilgjengeleg for alle utan særskilte tilgjengerettar.	Skal ikkje krevja innlogging eller annan form for identifikasjon, autentisering og autorisering. Integritet er viktig. Berre personar med rett tilgang kan endre dataa.
Intern	Einskilde arbeidsdokument, informasjon som er unnateke offentlegheit, einskilde personopplysningar, karakterar, studentarbeid, eksamenssvar/oppgåver, ikkje-publiserte forskingsdata- og arbeid.	Data som berre er rekna for tilsette, elevar ved VLFK eller namngjevne einskildpersonar eller grupper ved institusjonar VLFK samarbeider med.	Tilgjenge skjer etter innlogging med brukarnamn og passord.
Avgrensa	Einskilde strategidokument, sensitive personopplysningar, helseopplysningar, informasjon om sikring av bygningar og IT-system, eksamensoppgåver før dei er gitt, enkelte typar forskingsdata og -arbeider. Informasjon om personar som har adressesperre kode 7 eller som har behov for annan særleg beskyttelse.	Dette er informasjon som verksemda er pålagt å avgrensa tilgangen til i lov, føresegn, avtalar, reglement og anna regelverk. «Fortruleg» blir nytta viss det vil forårsaka skade for offentlege interesser, verksemda, einskildperson eller samarbeidspartnar om informasjonen blir kjent for uvedkommande.	Tilgjenge skjer etter innlogging med brukarnamn og passord. To-faktor autentisering ved bruk av sky-løysing. Berbare einingar: PC, Mac, USB-pinnar og -diskar må krypterast. Dokumenter som blir lagra i skya må merkast med etikettar/merkelappar.
Sensitive	Store mengder sensitive personopplysningar, store mengder helseopplysningar eller forskingsdata og datasett av stor økonomisk verdi. Informasjon om personar som har adressesperre kode 6 eller som har behov for annan særskilt vern.	Strengt fortruleg blir nytta viss det vil kunna forårsaka monaleg skade for offentlege interesser, institusjonen, einskildperson eller samarbeidspartnar at informasjonen blir kjent for uvedkommande. Informasjonen skal ha dei strengaste tilgjengerettar.	Plassering av data og informasjon i denne kategorien blir gjort i samarbeid med VLFK-juristar og IT-sikkerheitsteam.

I handboka blir det vist til eigne retningslinjer for klassifisering av informasjon. Revisjonen får i korrespondanse med fylkeskommunen opplyst at desse retningslinjene framleis ikkje er utarbeidd.

I utkast til dokumentet *IKT sikkerheitsarkitektur for Vestland fylkeskommune*,[33] går det fram at dei ovannemnde konfidensialitetsklassane har delvis korresponderande sonar i IKT-systemet i fylkeskommunen. Sonene er delt inn i *sikker*, *begrensa*, *intern* og *open sone*:

- ***Open sone*** korresponderer med *open* konfidensialitetsklasse. Her finn ein informasjon som skal eksponerast mot verda. Dette kan vere offisielle e-postar, fylkeskommunen sine opne websider og gjestenett.
- ***Intern sone*** korresponderer med delvis med både *intern* og *avgrensa* konfidensialitetsklasse. Her finn ein data som berre er meint for tilsette i fylkeskommunen, elevar eller andre namngjevne enkeltpersonar eller grupper i Vestland fylkeskommune. Døme på informasjon som er i intern sone inkluderer personopplysningar (som t.d. e-postadresse, bilnummer, IP-adresse, telefonnummer og fødselsdato), informasjon om karakterar og vitnemål, ein del HR-data (med unntak av HR-data klassifisert som begrensa eller sensitiv), eksamensopplysningar programvare/lisensinformasjon og systemdokumentasjon.
- ***Begrensa sone*** korresponderer delvis med konfidensialitetsklassen *avgrensa*. I denne sonen finn ein t.d. HR-data som er klassifisert som avgrensa, samt ein del annan informasjon i denne konfidensialitetsklassen.

[33] Dokumentet er datert 5. desember 2018, og er ikkje godkjent.

- ***Sikker sone*** korresponderer med konfidensialitetsklasse *sensitiv.* Her skal særlege kategoriar personopplysningar lagrast (t.d. personopplysningar om rase, medlemskap i fagforeining, helseopplysningar og politisk, filosofisk eller religiøs oppfatning), samt andre sensitive eller fortrulege opplysningar som hemmelege adresser, verksemdssensitiv informasjon mm.

I intervju får revisjonen opplyst at intern, avgrensa og sikker sone er sikra mot uautorisert tilgang. Vidare blir det opplyst at dei fleste informasjonssystema til Vestland fylkeskommune er plassert i avgrensa sone, med krav om to-faktor autentisering for pålogging.

4.4.2 Vurdering

Undersøkinga viser at det er iverksett tekniske og organisatoriske tiltak for å sikre at konfidensiell informasjon blir lagra trygt i Vestland fylkeskommune (sikker sone). Revisjonen meiner fylkeskommunen gjennom desse tiltaka langt på veg har sett i verk tilstrekkelege tiltak for at konfidensiell informasjon kan bli lagra trygt.

4.5 Kryptering av konfidensielle opplysningar

4.5.1 Datagrunnlag

I *Handbok for informasjonstryggleik og personvern i Vestland fylkeskommune* går det fram at det skal nyttast kryptografi for å verne informasjon i tråd med eigne retningslinjer. Revisjonen får opplyst at det ikkje er utarbeidd eigne rutinar eller prosedyrar for kryptering av konfidensielle opplysningar i Vestland fylkeskommune. I intervju blir det understreka at informasjon som er klassifisert som konfidensiell berre skal lagrast i *sikker sone*, og at det her er streng tilgangsstyring, både knytt til brukartilgangar og når det gjeld den tekniske infrastrukturen (linjene i sona er krypterte).

Dei tilsette i Vestland fylkeskommune er pålagde å ikkje lagre intern, konfidensiell eller sensitiv informasjon på flyttbare medium eller område som ikkje er sikra, med mindre informasjonen er kryptert (jf. *IT-sikkerheitsreglar for tilsette og eksterne i Vestland fylkeskommune)*. Vidare i reglementet går det fram at tilsette skal handtere sensitiv informasjon i system og filområde som er designa for lagring av slik informasjon. Revisjonen får opplyst at alle tilsette må lese og akseptere dette regelverket for å få tilgang til eiga datamaskin.

4.5.2 Vurdering

Undersøkinga viser at det er stilt krav om at konfidensiell informasjon som *ikkje* blir lagra trygt (sjå seksjon 4.4), skal krypterast. Det er ikkje utarbeidd rutinar eller prosedyrar for korleis slik kryptering skal skje. Revisjonen meiner dette er uheldig, då det kan bety at tilsette som lagrar konfidensiell informasjon utanfor sikker sone, ikkje er sett i stand til å ivareta kravet om at opplysningane då skal krypterast. Det er følgjeleg risiko for at konfidensielle opplysningar i Vestland fylkeskommune som ikkje blir lagra trygt, heller ikkje blir kryptert.

5. Tilgangsstyring

5.1 Problemstilling

I dette kapittelet vil vi svare på følgjande hovudproblemstilling med underproblemstillingar:

I kva grad har Vestland fylkeskommune etablert rutinar for tilgangsstyring, og i kva grad blir disse etterlevd?

Under dette:

a) Hindre uautorisert tilgang til informasjonssystema
b) Inn- og utmelding av tilsette i relevante informasjonssystema
c) Vurdering av om tilsette har riktige tilgangar i informasjonssystema
d) Loggføring av brukte tilgangar i informasjonssystema

5.2 Revisjonskriterium

Tilgjengelegheit er ein av dei grunnleggjande informasjonstryggleiksdimensjonane, saman med *integritet* og *konfidensialitet*. Å sørgje for *tilgjengelegheit* inneber å sikre tilgang til informasjon ved behov for tilgang, og sikre at det ikkje er informasjon ikkje er tilgjengeleg utan slikt behov. I ISO27001:2013 inneheld særleg kapittel 9 *Aksesskontroll*, inkludert seksjonane 9.2 *Styring av brukeraksess* og 9.4 *Kontroll av aksess til systemer og applikasjoner*, viktige retningslinjer for korleis sikre tilgjengelegheit. I seksjon 12.4 i ISO27001:2013 blir det òg stilt krav om logging i informasjonssystem, mellom anna for å beskytte mot misbruk og uautorisert tilgang.

Personvernforordninga artikkel 32 nr. 1 stiller krav om informasjonstryggleik ved behandling av personopplysningar. Krava som blir stilt er at man skal sette i verk egna tekniske og organisatoriske tiltak basert på risikovurderingar for å sikre vedvarande konfidensialitet, integritet, **tilgjengelegheit** og robustheit i behandlingsystema. Tiltak som også blir nemnd under artikkel 32 nr. 1 er pseudonymisering og kryptering av personopplysningar og evne til å rett opp igjen tilgjengelegheita og tilgangen til personopplysningar i rett tid dersom det oppstår ei fysisk eller teknisk hending.

Sjå vedlegg 2 for utfyllande revisjonskriterium.

5.3 Hindre uautorisert tilgang til informasjonssystema

Rutinar

Vestland fylkeskommune sitt styringssystem for informasjonstryggleik inneheld fleire dokument som tek føre seg tilgangsstyring. På overordna nivå går det i styringsdokumentet *Organisering av informasjons-sikkerheitsarbeidet* (nivå 1) fram at informasjon og infrastruktur skal klassifiserast med omsyn til tryggleiksnivå og tilgangsavgrensing. Det går vidare fram at det skal vere skriftlege retningslinjer for tilgangskontroll og passord som er basert på verksemds- og tryggleiksmessige krav og behov. I tillegg går det fram at det er systemeigar som skal definere kva for brukarar eller brukargruppe som skal ha tilgang til informasjon i eit informasjonssystem.

Også styringsdokumentet *Tilgangskontroll i Vestland fylkeskommune*[34] (nivå 2) er sentralt med omsyn til tilgangsstyringa i Vestland fylkeskommune. I dette dokumentet er mellom anna styrande prinsipp for tilgangsstyringa i Vestland fylkeskommune definert som følgjer:

1. ***Least privilege***: Ein skal ha minst mogleg tilgang, og all tilgang skal vere behovsbasert.
2. ***Eigarskap***: Systemeigar er ansvarleg for tilgangskontroll for sitt system.
3. ***Revisjon***: Alle tilgangar skal reviderast jamleg og skal følgje den tilsette i verksemda. Om ein tilsett bytter stilling eller om tilsettinga blir avslutta, skal unødige tilgangar og rettigheiter fjernast. Brukarkonto skal slettast etter avslutta stilling.
4. ***Administrator- og superbrukarkonto***: Talet på administrator- og superbrukarkonti i Vestland fylkeskommune skal minimerast i den grad det er mogleg utan å gå på akkord med funksjonalitet og evne til å utføre arbeid.

[34] Godkjent 12. oktober 2020.

5. ***Passord***: Alle brukare i Vestland fylkeskommune skal følgje Vestland fylkeskommune sin passord-policy. Ein skal nytte to-faktor autentisering der tenester eller data krev dette, og det lét seg gjennomføre i praksis.

All tilgangskontroll i Vestland fylkeskommune skal følgje desse prinsippa. Vidare går det fram i dokumentet at all tilgangskontroll i Vestland fylkeskommune skal dokumenterast, og alle førespurnader om nye tilgangar skal loggast i eit format som kan nyttast i revisjonar. Det skal ikkje vere mogleg å få nye tilgangar eller rettar i informasjonssystema basert på munnleg avtale.

Revisjonen har vidare fått tilsendt utkast til styringsdokumentet *Tilgangskontroll*.[35] Innhaldet supplerer *Tilgangskontroll*-dokumentet nemnd over, og går meir i detalj på korleis tilgangskontrollen i Vestland fylkeskommune skal gjennomførast praktisk og teknisk. I dokumentet går det fram at det er eit mål for Vestland fylkeskommune at tilgangskontrollen skal vere automatisk og kunne sporast, både med omsyn til oppretting av kontoar, samt i tildeling av tilgangsrettar. Vidare i dokumentet går det fram at Vestland fylkeskommune skal nytte brukaradministrasjonssystemet VIGO-BAS[36] både til oppretting, endring og stenging av brukarkontoar.

I utkast til dokumentet *IKT sikkerheitsarkitektur for Vestland fylkeskommune*,[37] er tilgangskontrollen til dei fire tryggleikssonene *open*, *intern*, *begrensa* og *sikker* skildra (sjå seksjon 4.4).

Praksis

I intervju blir det opplyst at mykje av den grunnleggande tilgangsstyringa i Vestland fylkeskommune i praksis er automatisert. Dei fleste relevante opplysninga om den enkelte tilsette er tilgjengeleg i HR-systemet til fylkeskommunen, t.d. kor i Vestland fylkeskommune dei arbeider, kva stilling dei har, og kor lenge kontrakten til førebels tilsette varer. Desse opplysningane er utgangspunktet for brukaroppretting, og er kopla til brukaradministrasjonssystemet VIGO-BAS, som igjen er kopla til tilgangsstyringssystemet Azure Active Directory (AD). Gjennom denne løysinga blir grunndata om den enkelte tilsette si stilling og arbeidsplass mm. nytta til å automatisk oppretta sentrale basistilgangar i dei største fagsystema (t.d. fellessystem som e-post, intranett, kvalitetssystem og HR-portal). Dei får då dei rette tilgangane for sin arbeidsplass og sitt stillingsnivå.

Tilgang til andre system enn desse basissystema må bestillast i samsvar med gjeldande retningslinjer og rutinar for den enkelte system. Desse retningslinjene og rutinane skal vere basert på prinsippa skildra i styringsdokumentet *Tilgangskontroll i Vestland fylkeskommune*. Vestland fylkeskommune søkjer vidare å sikre at nye informasjonssystem skal kunne koplast på den automatiserte løysinga for å sikre god tilgangsstyring. I *Retningslinjer for leverandørstyring og IT-anskaffingar*[38] går det fram at det er ønska at nye informasjonssystem har støtte for AD-integrasjon for tilgangsstyring.

Revisjonen får opplyst at nokre av felles- og fagsystema ikkje er ein del av denne automatiske prosedyren. I desse tilfella må leiarane gje tilgangar til eigne gruppeleiarar som igjen kan gi dei vidare til sine tilsette. Det er då eit leiaransvar å sikre tilgang til fagsystema. Manglande integrasjonar mellom systema gjer at ein kan oppleve forseinkingar i denne prosessen, til dømes når nytilsette skal få tilgang til systema. Revisjonen får opplyst at Vestland fylkeskommune er i prosess med å få på plass sjekklister knytt til dette, med mål om at organisasjonen er kjend med kva fristar som gjeld for at alt skal vere på plass til nytilsette har sin første arbeidsdag.

5.3.1 Vurdering

Vestland fylkeskommune har etablert rutinar for tilgangsstyring og for å hindre uautorisert tilgang til informasjonssystema. Revisjonen har ikkje avdekka noko som tilseier at desse rutinane ikkje er formålstenlege eller eigna til å hindre uautorisert tilgang til informasjonssystema. Fylkeskommunen har òg ein praksis på desse områda som langt på veg er automatisert, og som slik bidreg til å hindre uautorisert tilgang til mange av informasjonssystema.

Ikkje alle desse prosessane er automatiserte for alle informasjonssystema, noko som gjev auka risiko for svikt i tilgangsstyringa, og i neste runde også risiko for uautorisert tilgang til informasjonssystema. Det er

[35] Dokumentet er ikkje datert, men det går fram frå informasjon i dokumentet at det har vore under utarbeiding sidan mai 2019.
[36] VIGO-BAS er eit brukaradministrasjonssystem utvikla av VIGO IKS, for bruk i fylkeskommunar. Sjå: https://www.vigoiks.no/systeminformasjon/vigo-bas/om-vigo-bas-systemet
[37] Dokumentet er datert 5. desember 2018, og er ikkje godkjent.
[38] Vestland fylkeskommune. *Retningslinjer for leverandørstyring og IT-anskaffingar*. 10.08.2020

difor revisjonen si vurdering at Vestland fylkeskommune ikkje fullt ut har system, rutinar og praksis som hindrar uautorisert tilgang til informasjonssystema.

5.4 Inn- og utmelding av tilsette i informasjonssystema

5.4.1 Datagrunnlag

Rutinar

I tillegg til dei generelle tilgangsstyringsrutinane skildra i seksjon 5.3, er inn- og utmelding av tilsette i informasjonssystema i Vestland fylkeskommune kortfatta omtalt i *Handbok for informasjonssikkerheit og personvern i Vestland fylkeskommune*. Der går det fram at alle tilgangar skal reviderast og tilpassast ved endring i stilling/funksjon for ein tilsett. Det går òg fram at alle tilgangar skal avsluttast ved opphøyr av tilsetting. I sistnemnde situasjon vil brukaren først miste tilgang til sin AD-konto, og dermed også tilgang til dei fleste andre system.

Også i utkastet til dokumentet *Tilgangskontroll* er tilgangsstyring omtalt med omsyn til endring og avslutning av stilling. Mellom anna går det fram der at det ved opphøyr av stilling skal brukarkontoar deaktiverast og slettast etter 6 månadar.

Praksis

Revisjonen får opplyst at tilgangstyringa i dei største fagsystema er automatiske og at tilsette i Vestland fylkeskommune difor blir meldt inn i og ut av fagsystem etter kva stilling dei er registeret med i HR-systemet (sjå avsnittet *Praksis* i seksjon 5.3). I intervju blir det generelt vist til at risikoen for at tilsette ikkje har dei tilgangane dei skal ha, eller at tilsette som har slutta framleis har tilgangar til systema dei ikkje skal ha, er låg.

Det blir i intervju peikt på at det likevel er ein viss risiko for at tilsette som endrar jobb internt i Vestland fylkeskommune beheld tilgang til fagsystem knytt til tidlegare stilling dei ikkje lenger har tenestleg behov for. Dette skuldast at nokre av fagsystema som nemnd krev manuelle operasjonar for å avslutte tilgangar til tilsette som sluttar i stillinga si, og at dette ikkje alltid blir gjennomført ved endring av jobb internt. Det blir i intervju vist til konkrete tilfelle der tilsette har behaldt tilgangar etter bytte av stilling.

5.4.2 Vurdering

Undersøkinga viser at Vestland fylkeskommune har overordna rutinar og retningslinjer for inn- og utmelding av tilsette i informasjonssystema. Ikkje alle desse er ferdige eller godkjente, men overordna meiner revisjonen at innhaldet i rutinane tyder på at fylkeskommunen langt på veg har på plass eller er i prosess med å få på plass formålstenlege rutinar og retningslinjer på dette området.

Likevel er det revisjonen si vurdering er at rutinane for å sikre at tilsette som sluttar eller bytter avdeling internt i Vestland fylkeskommune berre i nokon grad er tilfredsstillande. Det at avslutning av tilgang i nokre fagsystem krev manuell operasjonar gjer at praksisen er sårbar og aukar risikoen for at tilsette som endrar stilling eller som har slutta, beheld tilgang til system dei ikkje treng.

5.5 Vurdering av riktige tilgangar til informasjonssystema

5.5.1 Datagrunnlag

Det er etablert rutinar og retningslinjer for vurdering av om tilsette har riktige tilgangar i informasjonssystema i Vestland fylkeskommune. I *Organisering av informasjonssikkerheitsarbeidet* går det fram at systemeigaren skal definere kva for brukarar eller brukargruppe som skal ha tilgang til informasjon og kva som er autorisert bruk av informasjonen. Systemeigar er bestillar/funksjonell premissgivar innan systemet sitt funksjonsområde (sjå tabell 2 i seksjon 3.4).

I *Handbok for informasjonssikkerheit og personvern i Vestland fylkeskommune* går det fram at Vestland fylkeskommune skal sikre at informasjon, data og program berre er tilgjengeleg for autoriserte personar.

I intervju blir det opplyst at det er systemeigar sitt ansvar å vurdere om tilsette har dei riktige tilgangane. Linjeleiarane må sende ei bestilling til systemeigar om kven som skal ha tilgang til kva. Det blir peikt på at ikkje alle systemeigarar er klar over dette ansvaret og at det er truleg er ein risiko for at tilsette har feil tilgangar i informasjonssystema.

Revisjonen får opplyst at det er etablert rutinar for gjennomgang av lister med oversikt over tilsette som har tilgang til dei mest kritiske systema. Til dømes gjennomfører linjeleiarane ein gjennomgang av tilsette som har tilgang til økonomisystema to gongar i året.

Vidare blir det peikt på at ein viktig del av arbeidet med tilgangar til informasjonssystema ikkje berre handlar om å avgrense tilgangar, men at dei tilsette må få tilgang til nødvendig informasjon for å gjennomføre sine arbeidsoppgåver.

I spørjeundersøkinga fekk respondentane spørsmål *om dei kjenner til område knytt til informasjons-tryggleik og/eller handsaming av personopplysningar der fylkeskommunen kan bli betre*. I fritekstfeltet for dette spørsmålet uttrykker nokre av dei tilsette at dei syns det er utfordrande å få tilgang til informasjon dei treng fordi ein ikkje har dei nødvendige verktøya eller dei nødvendige tilgangane.

5.5.2 Vurdering

Undersøkinga viser at det er etablert praksis å gjennomgå tilgangar til dei mest kritiske systema i Vestland fylkeskommune som til dømes økonomisystemet. Samtidig viser undersøkinga at tilgangstyring er systemeigarane i Vestland fylkeskommune sitt ansvar, og som tidlegare påpeikt er ikkje systemeigaransvaret klart for alle som har denne rolla. Dette medfører ein risiko for brot på informasjonstryggleiken i fylkeskommunen, særleg knytt til konfidensialitet og tilgjengelegheit.

5.6 Loggføring av brukte tilgangar

5.6.1 Datagrunnlag

Ingen av dokumenta som er tilgjengeleg for dei tilsette i kvalitetssystem til Vestland fylkeskommune tek føre seg rutinar og retningslinjer knytt til loggføring av brukte tilgangar.

Revisjonen har mottatt utkast til dokumentet *Hensiktsmessig logging* frå Vestland fylkeskommune. Formålet med dokumentet er å etablere hensiktsmessig logging i system som er nytta og/eller drifta av Vestland fylkeskommune, inkludert skytenester. Det går fram at fylkeskommunen frå eit tryggleiksorientert perspektiv ønskjer å lagre logger i 12 månadar eller meir for å kunne kartlegge hendingar som har skjedd over lang tid, men at Vestland fylkeskommune i praksis må vege behovet for tryggleik opp mot andre omsyn, som t.d. personvern o.l.

I intervju får revisjonen opplyst at brukte tilgangar i praksis blir logga i nokre fagsystem, og vidare at det for nokre av dei òg er etablert rutine for å gjennomgå desse loggane. I AD blir tilgangar gjennomgått årleg, og alle tilsette må då stadfeste at dei har lest og akseptert IT-reglementet (*IT-sikkerheitsreglar for tilsette og eksterne i Vestland fylkeskommune*) for å behalde tilgangen sin.

Systemeigarane som kan få tilgang til loggføring av brukte tilgangar i informasjonssystema dei er ansvarlege for og der slik logging i praksis blir gjort ved å etterspørje denne type rapportar frå IKT-seksjonen. Dette blir gjort i liten grad.

5.6.2 Vurdering

Undersøkinga viser at Vestland fylkeskommune ikkje har formelle rutinar for logging av brukte tilgangar i informasjonssystema. Revisjonen registrerer at slik logging i praksis skjer i nokre av informasjonssystema, og at for nokre av dei igjen blir loggane gjennomgått og kontrollert jamleg. Revisjonen meiner manglande rutinar – og eventuelt manglande moglegheit – for loggføring av brukte tilgangar i fylkeskommune sine informasjonssystem er uheldig. Det er òg uheldig om ikkje brukte tilgangar blir logga i alle systema som har moglegheit for det. Manglande loggføring av brukte tilgangar gjer at det ikkje er mogleg å avdekke eventuell uautorisert bruk av systema. Vidare meiner revisjonen at manglande praksis for å hente ut tilgangslogger frå system der slike blir eller kan produserast, også reduserer sannsynet for at eventuelle uautorisert bruk av desse systema blir avdekt. Manglande eller mangelfull logging og gjennomgang av slike er heller ikkje i samsvar med ISO27001:2013 punkt 12.4.

6. Personvern

6.1 Problemstilling

I dette kapittelet vil vi svare på følgjande hovudproblemstilling med underproblemstillingar:

I kva grad etterlever Vestland fylkeskommune sentrale krav i personvernlovgjevinga?

Under dette:

a) Har fylkeskommunen eit personvernombod med tilhøyrande ansvar og oppgåver som tilfredsstillar krava regelverket?
b) Fører fylkeskommunen protokoll over behandlingsaktivitetar av personopplysningar i samsvar med krava i regelverket?
c) Har fylkeskommunen personvernerklæring som følgjer krava i regelverket?
d) I kva grad blir det gjort risiko- og konsekvensvurderingar av handsaming av personopplysningar der det er krav om dette?
e) I kva grad har fylkeskommunen oversikt over avvik knytt til personvern, og i kva grad blir slike avvik meldt til Datatilsynet?

6.2 Revisjonskriterium

Personvernforordninga stiller krav om fylkeskommunen skal informere registrerte personar om at den handsamar personopplysningar om dei. Forordninga slår fast at informasjonen skal vere «kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk.» Datatilsynet skriv i sitt rettleiingsmateriell at ein behandlingsansvarleg t.d. etterkjem deler av informasjonskravet ved å ha ei personvernerklæring.

Personvernforordninga pålegg fylkeskommunen å utpeike eit personvernombod. Forordninga inneheld føresegner som regulerer stillingstilhøva for personvernombodet. Mellom anna skal fylkeskommunen sikre at personvernombodet blir involvert i rett tid i alle spørsmål som gjeld personopplysningar, at fylkeskommunen skal stille tilstrekkeleg ressursar til rådigheit for at personvernombodet kan gjennomføre oppgåvene pålagt stillinga i personvernforordninga, at personvernombodet skal vere uavhengig og rapportere direkte til fylkesrådmannen, og at personvernombodet er bunden av teieplikt. Personvernombodet sine lovpålagte oppgåver går fram av artikkel 39. Personvernombodet skal mellom anna skal kontrollere at personvernforordninga blir overhaldt, gi råd om vurdering av personvernkonsekvensar, og samarbeide med Datatilsynet.

Forordninga stiller vidare nye og skjerpa krav til kva avvik som skal meldast til Datatilsynet. Hovudregelen slik denne går fram i artikkel 33 er at alle avvik som skuldast brot på personopplysningstryggleiken (utilsikta sletting, tap, endring, ulovleg spreiing av eller tilgang til personopplysningar som er overført, lagra eller på anna måte handsama, jf. artikkel 4 punkt 12), skal meldast til Datatilsynet innan 72 timar.

Personvernforordninga stiller krav om at fylkeskommunen skal føre ein protokoll over behandlingsaktivitetane av personopplysingar som blir utført. Forordninga stiller nærare krav til innhaldet i protokollen, som t.d. namn og kontaktopplysning på den behandlingsansvarlege, formålet med behandlinga, ei skildring av kategoriane av registrerte og kategoriane av personopplysningar. Artikkelen stiller òg krav om at protokollen skal vere skriftleg og at protokollen skal gjerast tilgjengeleg for Datatilsynet dersom dei ber om det. Vidare stiller personvernforordninga krav om at fylkeskommunen skal ha skriftleg avtale med eventuelle databehandlarar som behandlar personopplysningar på fylkeskommunen sine vegner.

Forordninga stiller i tillegg krav om at det skal gjerast risikovurderingar av behandlinga av personopplysningar. Det er vidare eit krav at fylkeskommunen skal gjennomføre ei vurdering av personvernkonsekvensane av behandling av personopplysningar der slik behandling medfører høg risiko for rettar og fridom for fysiske personar. Jf. artikkel 39 om personvernombodet sine oppgåver, skal vedkomande gi råd om vurdering av personvernkonsekvensar og kontrollere gjennomføringa av denne dersom fylkeskommunen ber om det.

Sjå vedlegg 2 for utfyllande revisjonskriterium.

6.3 Personvernombod

6.3.1 Datagrunnlag

Vestland fylkeskommune har personvernombod. I samband med samanslåinga til Vestland fylkeskommune blei det tilsett eit felles personvernombod for HFK og SFFK, som òg skulle vere personvernombod for den nye fylkeskommunen. Vedkomande slutta i stillinga rett før etableringa av Vestland fylkeskommune, og fylkeskommunen har sidan då hatt periodar der stillinga har vore vakant, der ulike tilsette har vore konstituert i rolla. Det kjem fram i intervju at dette har ført til mindre kontinuitet i arbeidet knytt til etterleving av personvernregelverket.

Vestland fylkeskommune tilsette eit personvernombod i 50 % 17. august 2020. Det blir i nokre intervju peika på at ein stillingsbrøk på 50 % truleg ikkje er tilstrekkeleg for å handtere alle oppgåvene som ligg til rolla som personvernombod.

I det styrande dokumentet *Organisering av informasjonssikkerheitsarbeidet* går det fram at personvern-ombodet i Vestland fylkeskommune er rådgjevar for handsaming av personopplysningar og skal informere og gje råd knytt til behandling av personopplysningar. Personvernombodet skal også kontrollere at GDPR og verksemdas eigne retningslinjer for personvern blir etterlevd. Personvernombodet skal vidare svare på spørsmål knytt til behandling av personopplysningar, og om utøvinga av rettar i samsvar med personvernforordninga. Ombodet har mellom anna ha følgande oppgåver:

- Samle inn informasjon for å identifisere behandlingsaktivitetar
- Informere, gje råd og anbefalingar for å sikre regelverketterleving
- Gjennomføre haldningsskapande arbeid i verksemda knytt og opplæring av medarbeidarar
- Gje råd ved inngåing av leverandør- og databehandlaravtalar
- Samarbeide med datatilsynsmyndigheitene og fungere som eit kontaktpunkt, ref. førehandsdrøftingar Artikkel 36, for tilsynet ved spørsmål. Ved behov skal ombodet også kunne rådføre seg med tilsynet
- Ta omsyn til risikoen knytt til behandlingsaktivitetar sett i lys av handsamingas art, omfang, formål og samanhengen den utførast i. Personvernombodet skal difor prioritere innsatsen dit kor personvernrisikoen er høgast

Personvernombodet ligg organisatorisk under juridiske tenester i avdeling for organisasjon og økonomi. I same avdeling men under seksjon for HMT og kvalitetsstyring har Vestland fylkeskommune ein eigen personvernrådgjevarstilling med supplerande oppgåver til personvernombodet. Personvernrådgjevaren er fagansvarleg for personvern i fylkeskommunen og skal vere med å vidareutvikle styringssystemet for kvalitet og HMS, der personvern og informasjonstryggleik inngår som viktige tema. Ifølgje *Organisering av informasjonssikkerheitsarbeidet* skal personvernrådgjevaren mellom anna:

- Vidareutvikle rutinar for personvern og informasjonstryggleik.
- Vidareutvikle styringssystem for kvalitet på desse områda.
- Delta i arbeid med risikovurdering og kontinuitetsplanlegging.
- Vere pådrivar for gode og preventive handlingar for personvern og informasjonstryggleik.
- Sikre god informasjon til og opplæring av dei tilsette i fylkeskommunen.
- Generell rådgjeving og sakshandsaming, mellom anna i samband med IT-prosjekt og innkjøpsprosessar.

Stillinga som personvernrådgjevar er lyst fleire gonger. Det var ingen kvalifiserte søkjarar til denne stillinga etter førstegongsutlysing. Revisjonen får opplyst at det ved avslutninga av revisjonsperioden framleis ikkje var tilsett nokon i stillinga. På revisjonstidspunktet fungerte ein tilsett i fylkeskommunen som konstituert personvernrådgjevar.

I tillegg til personvernombod og personvernrådgjevar, har Vestland fylkeskommune som nemnd også ein IKT-sikkerheitsrådgjevar. Vedkomande har oppgåver som inneber koordinering, rådgjeving og kontroll av IKT-sikkerheitsarbeidet i organisasjonen, og har det faglege og praktiske ansvaret for utvikling og vedlikehald av styringssystemet for informasjonstryggleik. IKT-sikkerheitsrådgjevar skal mellom anna:

- Jobbe sektorovergripande saman med rådgjevar for beredskap, og inn mot seksjonane IKT og digitalisering.
- Gjennomføre og følgje opp tekniske ROS-vurderingar.

- Planlegge og gjennomføre aktivitetar knytt til informasjonssikkerheitsområdet; bidra til å bygge ein god sikkerheitskultur.
- Fortløpande vurdere potensielle sårbarheiter og rapportere til leiinga.
- Delta i utvikling av nye løysingar og kontinuerleg forbetring av eksisterande løysingar.
- Sørge for at dokumentasjon er på riktig nivå og oppdatert.
- Ansvar for implementering og vedlikehald av styringssystem for informasjonstryggleik.

I intervju blir det peikt på at denne organiseringa, der dei ulike rollane og oppgåvene ligg til ulike linjer, er formålstenleg mellom anna for å sikre naudsynt uavhengigheit. Det blir understreka som viktig at personvernombodet er lagt til ei eiga gruppa saman med dei andre ombodsfunksjonane for å tryggje den lovpålagte uavhengigheita, og elles at utarbeiding og drift av styringssystemet for informasjonstryggleik ikkje ligg til same eining som dei som skal ivareta den tekniske driftssida (seksjon IKT), og heller ikkje den strategiske digitaliseringssida (seksjon digitalisering).

6.3.2 Vurdering

Vestland fylkeskommune har eit personvernombod med tilhøyrande ansvar og oppgåver, samt stillingar som supplerer rolla til personvernombodet (personvernrådgjevar og IKT-sikkerheitsrådgjevar). Undersøkinga har ikkje avdekt noko som indikerer at mandatet til personvernombodet i Vestland fylkeskommune ikkje oppfyller krava i artikkel 39 i personvernforordringa. Samtidig viser undersøkinga at det har vore utfordringar knytt til utskiftingar av personar i stillinga som personvernombod. Revisjonen merkar seg òg at ein stillingsbrøk på 50 % blir vurdert som låg av fleire av dei intervjua sett opp mot oppgåvene og ansvaret som ligg til rolla.

6.4 Protokoll over behandlingsaktivitetar av personopplysningar

6.4.1 Datagrunnlag

Vestland fylkeskommune har reglar som seier at det skal førast protokoll over behandlingar av personopplysningar. Mellom anna går det i *Handbok for informasjonssikkerheit og personvern for Vestland fylkeskommune* frem at:

> VLFK skal ha eit oversyn over alle behandlingsaktivitetar ved behandling av personopplysningar. Forvaltning av informasjonseigedelar med personopplysningar skal inkludera protokoll over behandlingsaktivitetar som angjeve i GDPR Artikkel 30, og der kartlegging og dokumentasjon av behandlingsaktivitetar skal gjennomførast med eige godkjent skjema, og skal løpande haldast oppdatert. Det er kvar einskild eining sitt ansvar at protokollane kan dokumenterast og DPO [personvernombod] har høve til å føra kontroll med dette.

I utkast til *Rutine for ny behandling av personopplysningar* (omtala i 3.4) er det nærare skildra kven som har kva ansvar med omsyn til å føre protokoll over behandlingar av personopplysningar. Her går det fram at kvar eining/avdeling skal halde oversyn over pågåande behandlingar av personopplysningar, og at behandlingsprotokollen skal oppdaterast med nye behandlingar. Det går òg fram i utkast til rutinedokument at det skal vurderast om behandlinga av personopplysningar blir gjort av fylkeskommunen eller av ein databehandlar på vegner av fylkeskommunen, og i sistnemnde tilfelle, om det er inngått databehandlaravtale (sjå avsnitt *Databehandlaravtale* under).

Fylkeskommunen har utarbeidd mal for protokoll over behandlingar av personopplysningar. Malen er utarbeidd i Excel. Revisjonen har fått tilsendt tre versjonar av ein protokoll basert på denne malen med oversikt over behandlingar av personopplysningar. Protokollane er organisert dels etter verksemdprosessar (t.d. felles tekniske løysingar, ulike IT-verktøy), og dels etter funksjonar i organisasjonen (t.d. tannhelse, vidaregåande opplæring, næringsutvikling). Vidare har protokollane kolloner for kva system personopplysningane blir handsama i, om personopplysningane er regulære eller sensitive, kva som er formålet med behandlinga, kven som er system-/prosesseigar, kva behandlingsgrunnlag fylkeskommunen har,[39] om det er nytta databehandlar og om det er inngått databehandlaravtale (sjå avsnitt *Databehandlaravtale* under), kor mange det finnes personopplysningar om, kor lenge det er nødvendig å oppbevare opplysningane, osb.

Ingen av versjonane av protokollane revisjonen har motteke er fullstendige. Det er fylt ut nokre behandlingar for avdelingane for opplæring og kompetanse, tannhelse og eigedom, samt ein del på

[39] Det blir i intervju understreka at VLFK i dei fleste tilfelle har heimel i lov til å behandle personopplysningar.

overordna nivå. Det er ikkje fylt ut noko for avdelingane kultur, næringsutvikling, klima og miljø, administrasjon og organisasjon eller i kategorien ulike IT-verktøy.

I intervju går det fram at det i både tidlegare HFK og tidlegare SFFK blei arbeidd med å føre protokoll over system som behandla personopplysningar i organisasjonen, og at ein som følgje av har ein viss oversikt over behandlingar av personopplysningar, særleg i fylkesadministrasjonen og i skulesektoren i tidlegare HFK. Det blir samtidig peikt på at dokumenta ikkje har blitt jamleg oppdatert, at det er uklart kven som har ansvaret for å oppdatere protokollane, samt at det er uklart kor dei skal lagrast eller kven som skal følgje opp dette arbeidet.

I korrespondanse med fylkeskommunen får revisjonen opplyst at Vestland fylkeskommunen ikkje har oversikt over alle personopplysningane som blir behandla i fylkeskommunen. Vidare blir det opplyst at fleire av protokollane som finst for Vestland fylkeskommune er frå perioden 2018-2019, og stammar frå gamle Hordaland fylkeskommune. Arbeidet med å oppdatere og gjere desse protokollane fullstendige er påbegynt av personvernombodet, men er ikkje ferdig. Det blir vist til at det ikkje har vore og framleis ikkje er ressursar til å gjere ferdig dette arbeidet no. Det kjem òg tydeleg fram at Vestland fylkeskommune ikkje har protokollar for alle behandlingane av personopplysningar som blir gjennomført, og at det er forventa at dette først vil vere på plass våren 2021.

Databehandlaravtale

Som nemnd over inneheld både utkast til rutinedokumentet *Rutine for ny behandling av personopplysningar* og protokollmalen for behandling av personopplysningar punkt om databehandlaravtale. I tillegg er databehandlaravtalar omtalt i styringsdokumentet *Organisering av informasjonstryggleiksarbeidet*. Her går det fram det skal stillast krav om informasjonstryggleik når fylkeskommunen nyttar eksterne leverandørar for IKT-system, og at slike krav kan regulerast gjennom databehandlaravtale.

Revisjonen har vidare fått tilsendt utkast til sjekklista *Databehandlaravtalar - sjekkliste*.[40] Sjekklista skal nyttast for å gjennomgå eksisterande databehandlaravtale eller når databehandlaravtale skal inngåast med leverandør som behandlar personopplysningar på vegner av fylkeskommunen. Det går fram at det er behandlingsansvarleg som har ansvaret for at opplysningar behandlast i tråd med personopplysningslovens krav. Sjekklista tek føre seg krav om kva databehandlaravtalen skal innehalde i 11 punkt som skildring av pliktene til behandlingsansvarleg, pliktene til databehandlar og dei registrerte sine rettar. Det føreligg vidare eit vedlegg med 14 krav til informasjonstryggleik.

Vidare har det blitt utarbeidd ein *Mal for databehandlaravtalar.*[41] Denne malen er tilgjengeleg for det tilsette i kvalitetssystemet og tek føre seg mellom anna plikta til databehandlaren og rettane og pliktane til den behandlingsansvarlege. Malen skal tilpassast kvar enkelt avtale.

I korrespondanse med fylkeskommunen får revisjonen opplyst at det ikkje finst nokon samla oversikt over inngåtte databehandlaravtalar. Dette er eit arbeid personvernombodet skal starte opp saman med konstituert personvernsrådgjevar.

Revisjonen får i intervju opplyst at det på grunn av vakante stillingar i organisasjonen er ikkje ansvarsforholda knytt til databehandlaravtalar tydeleg. Som døme på dette blir det vist til at det tidvis har vore noko tilfeldig om personvernombodet har blitt kontakta om databehandlaravtalar i samband med innkjøp av nye IKT-system; i nokre tilfelle har personvernombodet blitt kontakta heilt i sluttfasen av innkjøpsprosessen og i mange saker blir ikkje personvernombodet kontakta i det heile tatt.

6.4.2 Vurdering

Vestland fylkeskommune stiller gjennom sitt styringssystem for informasjonstryggleik krav om at det skal bli ført protokoll over behandlingar av personopplysningar i samsvar med regelverket. Fylkeskommunen har òg utarbeidd utkast til rutinar for korleis delar av dette arbeidet skal gjennomførast, samt malar for slike protokollar. Fylkeskommunen har vidare begynt arbeidet med å føre slik protokoll over behandlingar av personopplysningar. Dette arbeidet var på revisjonstidspunktet ikkje ferdig. Fylkeskommunen bryt slik med kravet i personvernforordninga artikkel 30 nr. 1, om å føre protokoll over behandlingsaktivitetar av personopplysningar.

[40] Vestland fylkeskommune. *Databehandlaravtalar – sjekkliste*. Ikkje datert.
[41] Vestland fylkeskommune. *Databehandlaravtalemal*. Ikkje datert.

Vestland fylkeskommune har vidare etablert skriftlege rutinar for inngåing av databehandlaravtalar. Undersøkinga viser at fylkeskommunen ikkje har fullstendig oversikt over kva databehandlaravtalar som er inngått. Følgjeleg har dei heller ikkje oversikt over kva databehandlaravtalar som manglar. Revisjonen registrerer at det er pågåande arbeid med å etablere slik oversikt. På revisjonstidspunktet meiner revisjonen det er høg risiko for at fylkeskommunen ikkje oppfyller kravet i personvernforordninga artikkel 28 nr. 3 om å ha skriftlege avtalar med alle som behandlar personopplysningar på vegner av fylkeskommunen.

6.5 Personvernerklæring

6.5.1 Datagrunnlag

Vestland fylkeskommune har fleire personvernerklæringar som ligg på nettsida til fylkeskommunen under overskrifta «Personvern» på sida «Om oss»:

- *Personvernerklæring for vestlandfylke.no* (vlfk.no). Denne omhandlar korleis og kvifor fylkeskommunen samlar inn og brukar informasjon om besøkande på vestlandfylke.no.
- *Personvernerklæring for søkjarar og tilsette i fylkeskommunen.* Her går det mellom anna fram at kva opplysningar som blir registrert, korleis opplysningane blir behandla i samanheng med rekrutteringsprosessar, og meir generelt om behandling av personopplysningar og lagring av personopplysningar, inkludert med omsyn til rettsleg grunnlag for behandlingane, kor lenge personopplysningane blir lagra, og kva rettar registrerte har (m.a. innsyn, samtykke, retting, sletting).
- *Personvernerklæring for pasientar i tannhelsetenesta* inneheld mellom anna informasjon om korleis personopplysningar blir lagra, utlevering av person- og/eller helseopplysningar, samt rettane til pasienten (som mellom anna retten til å klage til datatilsynet).
- *Personvernerklæring – søknad om TT-kort i Vestland* inneheld informasjon om formål og rettsleg grunnlag for behandlinga, kva personopplysningar som blir behandla, samt rettane til den registrerte.

Personvernerklæringane på nettsida til fylkeskommunen har kontaktinformasjon til noverande personvernombod i Vestland fylkeskommune.

Revisjonen får vidare opplyst at Vestland fylkeskommune har utarbeidd personvernerklæringar for alle avdelingane i organisasjonen og at alle dei vidaregåande skulane har kvar si slik erklæring. I intervju blir det kommentert at fleire av personvernerklæringane er generelle, og det blir nemnd at det kunne vore hensiktsmessig å gjere dei meir konkrete inn mot avdelingane dei gjeld.

Revisjonen har gjort nokre oppslag på nettsidene til ulike vidaregåande skuler i fylket lenka frå vestlandfylkes.no for å undersøkje personvernerklæringane. Fleire av skulane har nettsider som ligg på dei gamle fylkeskommunane sine nettsider, med personvernerklæringar som òg stammar frå dei gamle fylkeskommunane (t.d. med tittel *Personvernerklæring for Sogn og Fjordane fylkeskommune sine nettstadar* som på Dale vidaregåande skule sine nettsider[42] eller med tilvising til fylkesrådmannen i HFK på Amalie Skram vidaregåande skule sine nettsider[43]). Kontaktinformasjon til personvernombodet i dei undersøkte personvernerklæringane var til det personvernombodet som var felles for Hordaland fylkeskommune og Sogn og Fjordane fylkeskommune.

6.5.2 Vurdering

Vestland fylkeskommune har fleire personvernerklæringar tilgjengeleg for publikum på sine nettsider. Det kjem ikkje fram informasjon knytt til dei fire personvernerklæringane som ligg på vestlandfylke.no som tyder på at desse ikkje er i samsvar med krava i personvernforordninga artikkel 12 nr. 1.

Det er heller ikkje indikasjonar som tyder på at personvernerklæringane som ligg på dei nettsidene til dei undersøkte skulane ikkje er i samsvar med krava i personvernforordninga. Det er likevel uheldig at desse har kontaktinformasjon til eit personvernombod som ikkje lenger er tilsett i fylkeskommunen, og elles har innhald som viser til dei førre fylkeskommunane.

6.6 Risikovurderingar knytt til handsaming av personopplysningar

6.6.1 Datagrunnlag

Vestland fylkeskommune har rutinar og prosedyrar for risikovurderingar knytt til handsaming av personopplysningar. Særleg sentral er seksjonen 1.4 Risikostyring i *Handbok for informasjonssikkerheit og*

[42] Sjå https://www.dale.vgs.no/personvernerklaering.466406.nn.html
[43] Sjå https://www.hordaland.no/nn-NO/skole/hfk-skole/personvernerklaring/

personvern for Vestland fylkeskommune. Her går det fram at Vestland fylkeskommune løypande skal analysera risiko og vurdere behovet for vernetiltak gjennom både regulære risiko- og sårbarheitsvurderingar (ROS) og meir omfattande personkonsekvensvurderingar (sokalla *Data Protection Impact Assessment* [DPIA]).

Vidare i handboka går det fram at tiltak for å redusere identifisert risiko skal vurderast med utgangspunkt i Vestland fylkeskommune si rolle som fylkeskommune og behandlar av personopplysningar og andre informasjonsverdiar, og at tiltak for å redusera risiko til et akseptabelt nivå skal ta omsyn til effektivitet, kostnad, moglegheiter og praktisk gjennomføring. Om ei risikovurdering avdekker uakseptabel risiko, skal det settast i verk tiltak for å redusere risikoen til eit akseptabelt nivå. Alle risikovurderingar skal i tillegg til å innehalda risikoreduserande tiltak, også fastsette ansvar og tidspunkt for gjennomføring av tiltak. Vidare skal alle risikovurderingar samlast og aggregerast i samla risikoregister. Revisjonen får opplyst at eit slikt register ikkje enno er på plass.

I handboka går det òg fram at det skal gjennomførast personvernkonsekvensvurdering (DPIA) der det ligg føre høg risiko for personopplysningsvernet, der det blir behandla sensitive personopplysningar (særskilte kategoriar av personopplysningar) eller ved behandling av personopplysningar i stor skala eller ved systematisk innsamling jf. GDPR artikkel 9, 35, betraktning 3. Personvernombodet (DPO) kan inkluderast i gjennomføring av personvernkonsekvensvurderingar (DPIA). I det styrande dokumentet *Organisering av informasjonssikkerheitsarbeidet* er det understreka at personvernombodet si rolle i gjennomføringa av DPIA er rådgjevande og kontrollerande, jf. personvernforordninga artikkel 35. Det er den behandlingsansvarlege, ikkje personvernombodet, som har ansvaret for slike vurderingar blir gjennomført.

Vidare går det fram i handboka at det minimum årleg skal gjennomførast ei overordna risikovurdering i Vestland fylkeskommune med omsyn til informasjonstryggleik og personvern. Det er IKT-sikkerheits-rådgjevar i Vestland fylkeskommune som er ansvarleg for at risikostyringsprosessane i Vestland fylkes-kommune blir koordinert i samsvar med desse vedtekne retningslinjer.

I utkast til *Rutine for ny behandling av personopplysningar* går det fram at den som har ansvaret for å ei ny behandling av personopplysningar skal sikre at det blir gjennomført risikovurderingar av behandlinga.

Revisjonen har òg fått tilsendt utkast til *Prosedyre for risikovurdering og PIA (personvern-konsekvensvurdering)*.[44] Prosedyren er ikkje tilpassa Vestland fylkeskommune, og er ikkje gjort tilgjengeleg verken i godkjent versjon eller utkastsform i kvalitetssystemet. Prosedyren gjer greie for korleis verksemda skal gjennomføre risikovurderingar av informasjonstryggleik og personvernkonsekvens-vurdering. Prosedyren skildrar mellom anna metode og utføring og mal for konsekvenstabell.

Revisjonen har fått tilsendt fleire ROS- og DPIA-vurderingar knytt til personvern gjennomført i 2019 og 2020.[45] Vurderingane er utarbeidd etter same mal og logikk; kvar behandlingsaktivitet i systema er vurdert med omsyn til risikoelement, manglar/svakheiter, og kva som er mogleg når det gjeld beskyttelse. Deretter følgjer risikoreduserande tiltak, med informasjon om kven som er ansvarleg og kva tid tiltaket skal gjennomførast. Og endeleg er det vurdert sannsyn og konsekvens for risikoelementet etter tiltaket er sett i verk, med samla restrisiko som eit produkt av sannsyn og konsekvens etter tiltak.[46]

I intervju får revisjonen opplyst at det er gjennomført ROS-vurderingar av behandlingar av person-opplysningar i alle system som har blitt etablert i samband med opprettinga av Vestland fylkeskommune, samt at slike vurderingar blir gjennomført ved nyanskaffingar og endringar i eksisterande system. Dette har bidratt til ein god oversikt over risikoane i desse systema. Det kan vere system frå dei gamle fylkeskommunane som framleis er i drift, som ikkje har blitt gjennomført risikovurderingar av dei siste par åra.

Det har også blitt gjennomført DPIA for tannhelse og skulesektoren i Vestland fylkeskommune. I intervju blir det peikt på at det er personavhengig om det blir gjennomført DPIA for personopplysningar i dei ulike

[44] Vestland fylkeskommune. *Prosedyre for risikovurdering og PIA (personvernkonsekvensvurdering).* Utkast. Dato: 21.02.2020

[45] Revisjonen har mottatt ROS- og DPIA-vurderingar som gjeld sakshandsamingssystemet ePhorte, mobil skule, det nye kvalitetssystemet, og opplæringssystemet KS læring. Revisjonen har òg fått tilsendt ein del andre meir generelle risikovurderingar av informasjonstryggleik til utvalde system. Desse er ikkje skildra her, då dei ikkje fokuserer på eller omhandlar personopplysningar.

[46] Kvalitetssystemet til fylkeskommunen har ein eigen risikomodul som nyleg er tatt i bruk. Etter det revisjonen kan sjå, er det ikkje gjennomført nokon fullstendig risikovurderingar i denne modulen.

avdelingane. Dei tilsette som kjenner til at dette skal gjennomførast tek kontakt med personvernombodet for rettleiing. Nokre avdelingar får hjelp av private advokatfirma til dette arbeidet. Til dømes har Skyss/Kringom utvikla eit verktøy for å undersøke kundetilfredsheit knytt til kollektivtransport. Her har eit privat advokatfirma gjennomført DPIA og ROS, og personvernombodet i Vestland fylkeskommune blei kopla på arbeidet med protokoll og personvernerklæring.

I korrespondanse med fylkeskommunen får revisjonen opplyst at det ikkje finst noko samla risikoregister for fylkeskommunen, men at dette er under utarbeiding av ekstern konsulent. Som nemnd over har risikovurderingar og personvernskonsekvensvurderingar i hovudsak har blitt gjennomført i samband med innkjøp av nye system. For eksisterande system, har det berre i nokon grad blitt gjort slike risikovurderingar. Forklaringa frå fylkeskommunen på dette er manglande kapasitet. I samband med verifiseringa av rapporten, understrekar fylkeskommunen at dei har ei større samling risikovurderingar tilgjengeleg på eit fellesområde.[47]

6.6.2 Vurdering

Vestland fylkeskommune har etablert rutinar for gjennomføring av risikovurderingar knytt til behandling av personopplysningar og personvernkonsensvurderingar (DPIA), og har vidare ytterlegare rutinar under utarbeiding. Undersøkinga viser òg at det har blitt gjennomført nokre slike risikovurderingar, men at desse i hovudsak har vært gjort for behandlingar av personopplysningar i nye system; for eksisterande system har det ikkje eller berre i nokon grad blitt gjort risikovurdert knytt til behandling av personopplysningar eller personvernkonsekvensvurderingar. Revisjonen er merksam på at rutinane for slike vurderingar er relativt nyleg utarbeidd og at nokre av dei framleis er under utarbeiding. Vi merkar oss òg at manglande kapasitet blir oppgjeve som hovudforklaring på manglande risikovurderingar av behandlingar av personopplysningar i eldre system. Manglande risikovurderingar av behandlingar av personopplysningar betyr at Vestland fylkeskommune bryt med personvernforordninga artikkel 32 nr. 1.

Undersøkinga viser vidare at fylkeskommunen ikkje har noko risikoregisert med oversikt over kva system og behandlingar av personopplysningar som er risikovurdert, og kva som ikkje er risikovurdert. Revisjonen er merksam på at det har blitt gjennomført fleire risikovurderingar, og at fylkeskommunen har desse samla. Likevel meiner vi at det er uheldig at fylkeskommunen ikkje har oversikt over kva som er gjort og kva som står att med omsyn til risikovurderingar av behandlingar av personopplysningar. Sett i samanheng med at fylkeskommunen heller ikkje har nokon oversikt over kva behandlingar av personopplysningar som blir gjort, jf. avsnitt 6.4.2, har fylkeskommunen heller ikkje full oversikt over kor det er eller kan vere personvernrisikoar. Fylkeskommunen har difor heller ikkje full oversikt over kva eventuelle tryggleikstiltak som fungerer og kva tryggleikstiltak som ikkje fungerer. Fylkeskommunen manglar med dette grunnlag for å gjere eventuelle justeringar og slik kontinuerleg forbetre informasjonstryggleiken. Manglande oversikt over behandlingar av personopplysningar og manglande risikovurderingar av slike behandlingar, betyr vidare at fylkeskommunen heller ikkje har fullstendig oversikt over kva personopplysningar dei handsamar som har høg risiko, og fylkeskommunen har difor heller ikkje grunnlag for å gjennomføre vurdering av personvernkonsekvensar ved behandling av personopplysningar med høg risiko, jf. personvernforordninga artikkel 35.

6.7 Avvik og avviksmelding til Datatilsynet

6.7.1 Datagrunnlag

Vestland fylkeskommune har gjennom sitt styringssystem for informasjonstryggleik retningslinjer og rutinar for melding av avvik. I det styrande dokumentet *Organisering av informasjonssikkerheitsarbeidet* blir det slått fast at alle tryggleiksbrot, samt all bruk av informasjonssystem i strid med fastlagde rutinar, skal handterast som avvik. Også i *IT-sikkerheitsreglar for tilsette og eksterne i Vestland fylkeskommune* går det fram at alle avvik skal meldast; det går der fram at alle tilsette i fylkeskommunen skal stadfeste at dei melder avvik dersom dei opplever at nokon bryt tryggleiksreglane, eller oppdagar andre alvorlege brot på konfidensialitet, integritet eller tilgjenge. Det er i reglementet vist til avviksprosedyren i kvalitetssystemet for nærare informasjon. Også dokumenta *Etterleving av informasjonssikkerheit i VLFK* og *Handbok for informasjonssikkerheit og personvern i Vestland fylkeskommune* omhandlar avvik, både med omsyn til kva som er rekna som eit avvik (brot på interne reglar og rutinar for informasjonstryggleik

[47] Risikovurderingane er samla i ei Microsoft Teams-gruppe.

og personvern, og/eller brot på integritet, konfidensialitet, tilgjengelegheit eller personvern), og at ein kvar brukar av informasjonssystema er ansvarleg for å rapportere brot og moglege brot på tryggleiken.

Sjølve avviksprosedyren (dokumentet *Avviksbehandling*[48]) er ei generell prosedyre for all avviksmelding i fylkeskommunen, og inngår ikkje i styringssystemet for informasjonstryggleik. Rutinen har eit eiget avsnitt som tek føre seg prosedyrar ved registrering og sending av avvik knytt til informasjonstryggleik og personvern. Det går fram at meldar av avvik skal bruke kategorien «Informasjonssikkerheit, personvern» i avviksystemet som er ein modul i kvalitetssystemet.[49] Når varselet er lagra i avvikssystemet blir avviket automatisk sendt til eigne saksbehandlarar for personvern og til personvernombodet.[50] Saksbehandlar skal raskt avgjere om avviket er så alvorleg at det må sendast særskilt melding til Datatilsynet. Dette skal i tilfelle skje innan 72 timar. Elles følgjer avvikshandsaminga for informasjonstryggleiks- og personvernavvik dei same reglane som andre avvik i fylkeskommunen; næraste leiar har ansvar for å følgje opp avviket. Skjer ikkje dette innan fem dagar, blir avviket eskalert til neste nivå i organisasjonen. Når avviket er ferdig behandla, t.d. ved at oppgåver og tiltak er gjennomført, skal avviket lukkast. Det må då skrivast ein konklusjon, og det skal bli gitt beskjed til den som registrerte avviket om kva som er gjort for å lukke avviket.

I kvalitetssystemet går det fram at det frå 1. januar 2020 til 19. oktober 2020 er meldt 10 avvik knytt til informasjonstryggleik i Vestland fylkeskommune. Av desse ti er eitt avvik vurdert som å ha høg alvorlegheitsgrad, tre middels alvorlegheitsgrad, fire som låg alvorlegheitsgrad, og for to er dette ikkje vurdert. Seks av avvika er lukka, medan dei fire resterande ikkje er lukka. I intervju får revisjonen opplyst at to av avvika er meldt vidare til Datatilsynet, og at desse skal vere blant dei lukka avvika. Av dei fire som ikkje er lukka, ble to meldt i mai 2020.

Det blir i intervju peika på fleire forklaringar for kvifor det ikkje blir meldt fleire avvik i Vestland fylkeskommune. Mellom anna blir innføringa av nytt kvalitetssystem samt manglande kjennskap til avvikssystemet nemnd som viktige årsaker av fleire. Vidare blir det peika på at leiarane som mottek avvika ikkje i tilstrekkeleg grad er kjende med korleis dei skal lukke avvik, noko som kan gjere motivasjonen for å melde avvik lågare. Fleire fortel også at dei tilsette i Vestland fylkeskommune er generelt usikre på kva som reknast som avvik og er dermed usikre på kva som skal meldast. Særleg er det knytt usikkerheit til kva avvik som er knytt til IKT og kva som er som knytt til personvernreglementet. Det blir vidare kommentert i intervju at tilsette truleg heller kontaktar IKT-avdelinga pr. telefon enn å melde frå om avvik i kvalitetssystemet. I tillegg går det fram i intervju at avviksystema i tidlegare SFFK og HFK heller ikkje blei nytta i særleg grad til å melde avvik om informasjonstryggleik.

I spørjeundersøkinga går det fram at mange tilsette ikkje er kjende med rutinane for å melde avvik og at avvik som gjeld informasjonstryggleik ofte ikkje blir meldt (sjå kapittel 7).

6.7.2 Vurdering

Vestland fylkeskommune har etablert rutinar for avviksmelding som mellom anna seier at personvernavvik skal meldast til Datatilsynet innan 72, timar, slik det er stilt krav om i personvernforordninga.

Vestland fylkeskommune har vidare eit avviksystem tilgjengeleg for alle tilsette, og undersøkinga viser at det blir meldt avvik knytt til informasjonstryggleik i dette. Svara i spørjeundersøkinga tyder på at ikkje alle tilsette i fylkeskommunen veit at dei skal melde avvik knytt til informasjonstryggleik når dei opplever eller observerer slike. Dette gjev risiko for at avvik ikkje blir meldt, og både svara i spørjeundersøkinga, informasjon frå intervju og talet informasjonstryggleiksavvik meldt i avviksystemet tyder på at denne risikoen har gjort seg gjeldande i fylkeskommunen. Revisjonen vil i den samanheng peike på at manglande avviksmeldingar aukar risikoen for at svakheiter i systema ikkje blir retta. Revisjonen meiner at fylkeskommunen sin avvikspraksis ikkje er i samsvar med tilrådingane i ISO27001:2013 eller generelle prinsipp for god internkontroll.

[48] Vestland fylkeskommune. *Avviksbehandling.* Dato: 01.04.2020
[49] Avviksystemet der tilsette i Vestland fylkeskommune skal melde avvik blei gjort tilgjengeleg i januar 2020. Systemet er ein modul i kvalitetssystemet.
[50] Saksbehandlar for personvern kan vere t.d. personvernrådgjevar, informasjonssikkerheitsrådgivar eller annan kompetent rådgjevar som blir peikt ut av fylkesdirektør organisasjon og økonomi.

7. Kompetanse om informasjonstryggleik

7.1 Problemstilling

I dette kapittelet vil vi svare på følgjande hovudproblemstilling med underproblemstillingar:

I kva grad har dei tilsette i fylkeskommunen tilstrekkeleg kompetanse om informasjonstryggleik?

Under dette:

a) Er det etablert rutinar for å gje tilsette opplæring i informasjonstryggleik?
b) I kva grad har dei tilsette kjennskap til ev. retningslinjer og rutinar for informasjonstryggleik?
c) I kva grad blir ev. retningslinjer og rutinar for informasjonstryggleik følgt?

7.2 Revisjonskriterium

Fylkeskommunen er i eForvaltningsforskrifta § 15 forplikta til å ha ein internkontroll basert på anerkjende standardar for styringssystem for informasjonstryggleik. Departementet har peika ut direktorat for forvaltning og IKT (Difi) som ansvarleg for å gje tilrådingar knytt til kva styringssystem for informasjonstryggleik som bør nyttast, og Difi tilrår at offentlege verksemder baserer seg på ISO/IEC 27001:2013. Kapittel 7.2 i standarden seier at fylkeskommunen skal:

> a) fastslå hvilken kompetanse som er nødvendig for personen(e) som utfører arbeid under organisasjonens styring, og som påvirker dens informasjonssikkerhetsprestasjon;
>
> b) sikre at disse personene har kompetanse tilegnet gjennom passende utdanning, opplæring eller erfaring;
>
> c) der det er relevant, treffe tiltak for å erverve nødvendig kompetanse og evaluere virkningen av tiltakene som er truffet; og
>
> d) oppbevare relevant dokumentert informasjon som bevis på kompetanse.

I merknaden til punkt 7.2, står det at «Aktuelle tiltak kan for eksempel omfatte å sørge for opplæring, veiledning eller omplassering av nåværende ansatte eller innleie av eller kontraktinngåelse med kompetente personer.»

I Datatilsynet sin rettleiar Internkontroll og informasjonssikkerhet[51] omhandlar mellom anna oppfølging og opplæring. Her går det fram at målet med brukaropplæring er å syte for at brukarane er merksame på truslar mot personvernet og informasjonstryggleiken generelt, og at dei er gitt høve til å etterleve dette i sitt daglege arbeid. Opplæringa bør vere tilpassa dei ulike målgruppene sitt behov for opplæring og fordelast over tid. Brukarane bør få opplæring i rutinar, tryggleiksprosedyrar og riktig bruk av informasjonssystem for å redusere potensielle risikoar.

I tillegg til tilrådinga om opplæring av tilsette som følgjer av ISO-standarden, kan ein utleie eit krav om opplæring og kjennskap til system, rutinar og regelverk blant tilsette frå kommunelova § 31-3 a), som seier at fylkesrådmannen skal «sørge for at administrasjonen er gjenstand for betryggende kontroll.» Denne paragrafen er ei overgangsbestemming fram til internkontrollføresegna i kapittel 25 i kommunelova trer i kraft 1. januar 2021. Fylkesrådmannen skal med andre ord sikre intern kontroll med forvaltninga si. Eit sentralt tiltak i eitkvart internkontrollsystem vil vere at det er på plass tilstrekkeleg opplæring til at dei tilsette er i stand til å gjennomføre sine arbeidsoppgåver i samsvar med lover, krav og forventningar.

Sjå vedlegg 2 for utfyllande revisjonskriterium.

[51] *Internkontroll og informasjonssikkerhet.* Datatilsynet. Publisert 23.06.2018. https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/

7.3 Rutinar for opplæring i informasjonstryggleik

7.3.1 Datagrunnlag

Vestland fylkeskommune stiller gjennom sitt styringssystem for informasjonstryggleik krav om at tilsette skal få opplæring i informasjonstryggleik. I det styrande dokumentet *Organisering av informasjons-sikkerheitsarbeidet* (nivå 1) står det at fylkesrådmannen «skal sørge for at det blir lagt til rette for at alle brukarar får naudsynt opplæring og materiell, slik at brukarane kan verne VLFK sin informasjon og informasjonssystem». Den praktiske gjennomføringa av opplæringa er fordelt mellom linjeleiarane, IKT-sikkerheitsrådgjevar, personvernombod og personvernrådgjevar; linjeleiarane skal sørgje for at eige personell gjennomfører grunnleggande opplæring, IKT-sikkerheitsrådgjevar har fullmakt til å foreslå og gjennomføre opplæring i informasjonstryggleik, personvernombodet skal gjennomføre haldningsskapande arbeid i verksemda og opplæring av medarbeidarar, og personvernrådgjevaren skal gi informasjon til og opplæring av dei tilsette i fylkeskommunen.

Også *Handbok for informasjonssikkerheit og personvern for Vestland fylkeskommune* (nivå 2) inneheld reglar og retningslinjer for opplæring av tilsette innanfor informasjonstryggleik. Det går der mellom anna fram at Vestland fylkeskommune skal fastslå kva for kompetanse som er naudsynt for personane som arbeider i og for fylkeskommunen, og som har betyding med omsyn til personvern og informasjons-tryggleik. Vidare skal Vestland fylkeskommune sikre at desse personane har denne kompetansen tileigna gjennom passande utdanning, opplæring eller erfaring. I tillegg står det at Vestland fylkeskommune skal oppbevara dokumentert informasjon som prov på kompetanse.

Som tidlegare nemnd skal alle tilsette og innleigde i Vestland fylkeskommune signere lese og akseptere reglementet *IT-sikkerheitsreglar for tilsette og eksterne i Vestland fylkeskommune*. I dette går det frem fleire vesentlege punkt knytt til informasjonstryggleik, som t.d. kva den tilsette er ansvarleg for (m.a. beskytte data, etterleve rutinar og reglar, melde avvik), at dei ikkje skal dele passord, at dei skal låse maskina når den ikkje er i bruk, osb.

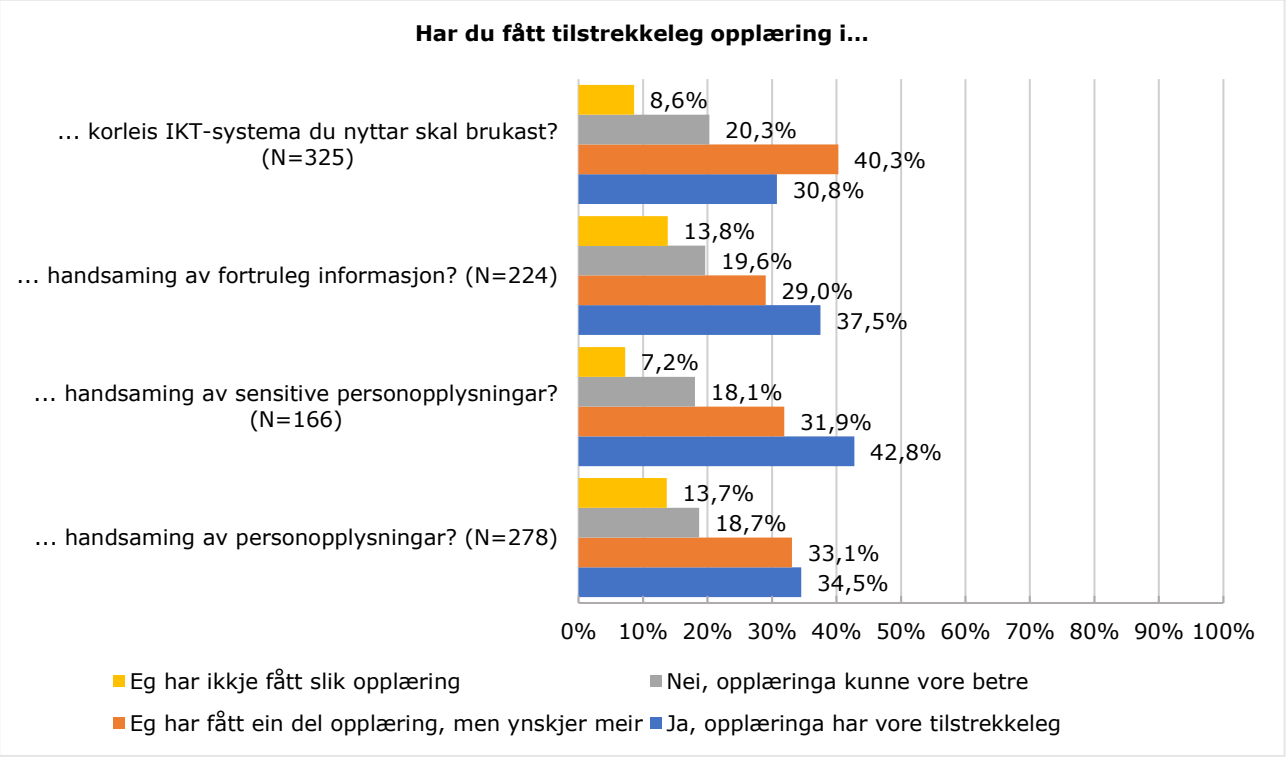
I korrespondanse med fylkeskommunen får revisjonen opplyst at det ikkje har vore gitt faktisk opplæring til tilsette i Vestland fylkeskommunen innan informasjonstryggleik sidan etableringa av fylkeskommunen. Dette blir òg stadfesta i intervjua. I intervju blir det vist til at manglande opplæring på området mellom anna skuldast at styringssystemet for informasjonstryggleik framleis er under utarbeiding, og at mange av prosedyrane, rutinane og retningslinjene det skal gis opplæring i ikkje finst enno. Vidare blir det peikt på at organisasjonen framleis er ny, og at COVID-19-pandemien har hatt konsekvensar for i kva grad ein har hatt moglegheit til å arbeide med kompetansetiltak på dette området.

Det blir likevel vist til nokre konkrete døme på kompetansehevingstiltak innanfor informasjonstryggleik som har blitt gjennomført. Til dømes blei informasjonstryggleik tematisert på eit allmøte i samband med overgangen til nytt IKT-system. Det blei også sendt ut ein informasjonstryggleikvideo til alle tilsette i organisasjonen i samband med samanslåing til Vestland fylkeskommune. Det har vidare blitt arrangert ei personvernsamling for fylkesdirektørar og seksjonsleiarar i organisasjonen, der mellom anna databehandlaravtalar og avviksrapportering var tema. Samlinga var også ope for tilsette som ikkje har leiarstilling, men som har sentrale roller der informasjonstryggleik står sentralt. I samlinga var det leigd inn ekstern føredragshaldar.

I intervju blir det også vist til at det har vore sporadisk oppslag på intranettet til fylkeskommunen knytt til informasjonstryggleik. IKT-sikkerheitsrådgjevar har også oppretta ei «sikkerheitsside» med informasjon på intranettet til fylkeskommunen som er tilgjengeleg for alle tilsette. På denne sida ligg det lenkjer med kurs i regi av KS både for tilsette og leiarar og for personar som arbeider med personopplysningar. På forsida blir det kort gjort greie for korleis ein arbeider med tryggleik i Vestland fylkeskommune, kva det betyr for den enkelte tilsette og kvifor dette er viktig for Vestland fylkeskommune. Vidare er det lagt inn fleire brukarrettleiingar, som t.d. korleis endre passord, korleis sjekke søppelpost, og korleis skanne for virus. Kontaktinformasjon til IKT-sikkerheitsrådgjevar og personvernombodet er også opplyst om på sida.

I spørjeundersøkinga fekk alle respondentane spørsmål om mottatt opplæring knytt til informasjons-tryggleik og personvern. Svara går fram i figur 5 under:

Figur 5: Opplæring knytt til fortruleg informasjon



Som figur 5 viser, svara mellom 30,8 % og 42,8 % at dei har fått tilstrekkeleg opplæring innanfor viktige informasjonstryggleiksområder; 8 % og 14 % av respondentane svara at dei ikkje har fått slik opplæring i det heile, mellom 29 % og 40 % svara at dei har fått ein del opplæring, men ynskjer meir, og mellom 18 % og 20 % svara at opplæringa kunne vore betre.

Alle som svarte at dei ynskjer meir opplæring fekk eit oppfølgingsspørsmål om *kva opplæring knytt til informasjonstryggleik og/eller bruk av IKT-system dei saknar.* Av dei 141 som svara peikte mange på behov for opplæring informasjonstryggleik generelt gjerne via kurs, opplæring for innformasjonstryggleik knytt til deira eigne arbeidsoppgåver, samt opplæring i avvikmelding og avvikshandtering. Fleire uttrykkjer også at det med fordel kunne vore lettare å finne rutinane Vestland fylkeskommune har som gjeld informasjonstryggleik. Vidare blir det vist til behov for opplæring i sakshandsamingssystemet ePhorte og korleis ein i dette systemet skal sikre informasjonstryggleik. Fleire skriv også at dei ynskjer oppfrisking i kunnskap, då det går lenge mellom kvar gong dei handterer personopplysningar.

Respondentane i spørjeundersøkinga som svara at dei er systemeigarar fekk spørsmål *om dei har deltatt i opplæringa av andre brukarar.* 66,7 % svara «ja», og dei resterande 33,3 % svara «nei» på dette spørsmålet.[52]

7.3.2 Vurdering

Vestland fylkeskommune har gjennom dei delane av styringssystemet for informasjonstryggleik som er ferdig, plassert ansvar og oppgåver knytt til opplæring innanfor informasjonstryggleik. Vidare skal alle tilsette i Vestland fylkeskommune vere informert om grunnleggjande informasjonstryggleikskrav gjennom internt regelverk. Både delane av styringssystemet som er ferdig og det aktuelle regelverket er nyleg utarbeidd og godkjent. Fylkeskommunen er vidare open på at opplæring av tilsette ikkje har blitt prioritert før organisasjonen har gjort ferdig nødvendig dokumentasjon i styringssystemet, og at det difor ikkje har blitt gitt systematisk opplæring på dette området. Det er heller ikkje lagt konkrete planar for korleis slik opplæring skal bli gitt.

Det kjem også fram i undersøkinga at nesten 70 % av respondentane i spørjeundersøkinga ikkje har fått tilstrekkeleg opplæring bruk av IT-systema, 65,5 % ikkje har fått tilstrekkeleg opplæring i handsaming av personopplysningar, ca. 57 % ikkje har fått tilstrekkeleg opplæring i handsaming av sensitive

[52] N=21

personopplysningar, og 62,5 % ikkje har fått tilstrekkeleg opplæring i handsaming av fortruleg informasjon. Revisjonen meiner difor at fylkeskommune på revisjonstidspunktet ikkje har sikra at dei tilsette får naudsynt opplæring i informasjonstryggleik på revisjonstidspunktet.

Det er følgjeleg revisjonen si vurdering at Vestland fylkeskommune ikkje oppfyller krav og anbefalingar knytt til å sikre tilstrekkeleg informasjonstryggleikskompetanse blant dei tilsette gjennom opplæringstiltak (t.d. ISO27001:2013 punkt 7.2). Dette gjer at det er høgare sannsyn for at dei tilsette ikkje har tilstrekkeleg kompetanse innan informasjonstryggleik, noko som aukar risiko for brot på regelverket som gjeld for behandling av personopplysningar og informasjonstryggleiken generelt.

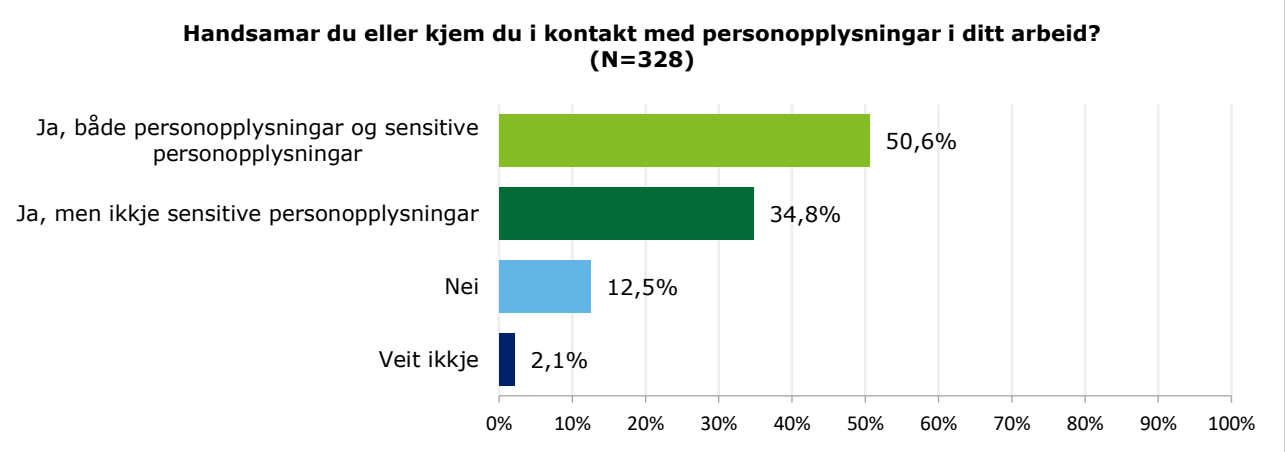
7.4 Kjennskap til retningslinjer og rutinar for informasjonstryggleik

7.4.1 Datagrunnlag

Som skildra i seksjon 7.3, har det ikkje blitt gjennomført systematiske opplæringstiltak knytt til informasjonstryggleik i Vestland fylkeskommune. Revisjonen får vidare opplyst det heller ikkje er gjennomført dokumentert opplæring av dei tilsette i gjeldande retningslinjer eller rutinar for informasjonstryggleik i fylkeskommunen. I intervju blir det gjennomgåande vist til at tilsette i Vestland fylkeskommune sin informasjonstryggleikspraksis nok ikkje er tilfredsstillande, og at opplæring av tilsette er heilt sentralt for å klare å etablere ein vellukka tryggleikskultur når styringssystemet er klart.

I spørjeundersøkinga som blei gjennomført i samband med forvaltningsrevisjonen blei respondentane bedne om å svare på ei rekkje spørsmål med relevans for kompetanse og opplæring innanfor informasjonstryggleik. Innleiingsvis blei det spurt om dei *handsamar eller kjem i kontakt med personopplysningar* som del av sitt arbeid. Som vist i figur 6 svara til saman 85,4 % av dei 328 respondentane i spørjeundersøkinga at dei *handsamar eller kjem i kontakt med berre personopplysningar* (34,8 %) eller *både personopplysningar og sensitive personopplysningar* (50,6 %). På spørsmål om dei *handsamar eller kjem i kontakt med anna fortruleg informasjon som følgje av sitt arbeid*, svara 68,9 % «ja».[53]

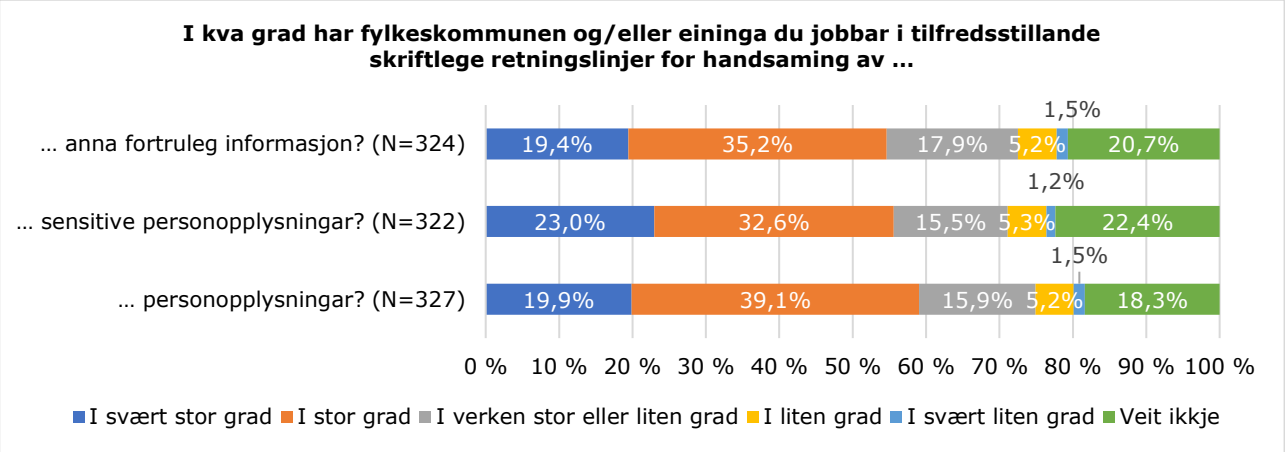
Figur 6: Behandling av personopplysningar



Respondentane blei vidare spurde om i *kva grad fylkeskommunen og/eller einingа vedkommande jobbar i har tydelege og skriftlege retningslinjer for handsaming av ulike typar opplysningar.* Som det går fram i figur 7 svara mellom 18 % og 23 % «veit ikkje», litt over 5 % «i liten grad» og om lag 1,5 % «i svært liten grad».

[53] N=328

Figur 7: Retningslinjer for handsaming av personopplysningar og fortruleg informasjon

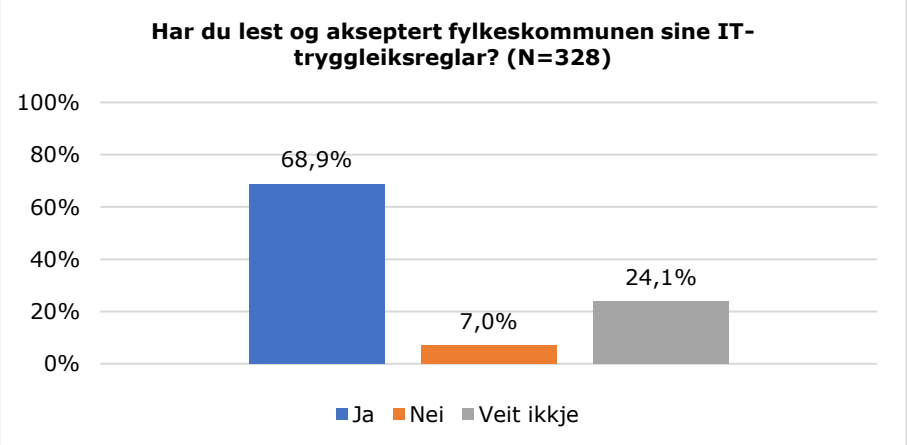


Respondentane som anten svara «i svært stor grad» eller «i stor grad» på spørsmålet over, blei spurde om dei *veit kvar dei finn rutinar og retningslinjer for handsaming av personopplysningar, sensitive personopplysningar og/eller anna fortruleg informasjon som gjeld fylkeskommunen og/eller di eining*. På dette svara 67,5 % «ja» og 32,5 % «nei».[54] Dei som svara «ja» blei så spurde om *kvar* dei finn slike rutinar og retningslinjer; av dei 131 som fekk dette spørsmålet, svara 115, og av desse svara langt dei fleste at dei finn slike rutinar og retningslinjer i fylkeskommunen sitt kvalitetssystem. Nokre viste òg til lovverket, at dei har fått tilsendt retningslinjer per e-post, at dei har fått munnleg informasjon, eller dei viste til sektorspesifikke intranettsider (t.d. innanfor skule).

Respondentane fekk òg spørsmål om dei har signert fylkeskommunen si fråsegn om teieplikt; 68,7 % svara «ja», 8,6 % svara «nei» og 21,7 % svara «veit ikkje». Dei som svara «ja» på at dei har underteikna fylkeskommunen si fråsegn om teieplikt blei spurde om *i kva grad dei hugsar innhaldet i teiepliktskjema.* Om lag ein fjerdedel (25,7 %) svarte «i verken stor eller liten grad» på dette, medan 8,4 % svara «i liten grad».[55]

Som det går fram i figur 8 svara langt dei fleste at dei har lest og akseptert fylkeskommunen sine IT-tryggleiksreglar. Samtidig svara 7 % «nei» og om lag 24 % svara «veit ikkje» på spørsmålet.

Figur 8: Kjennskap til IT-tryggleiksreglar

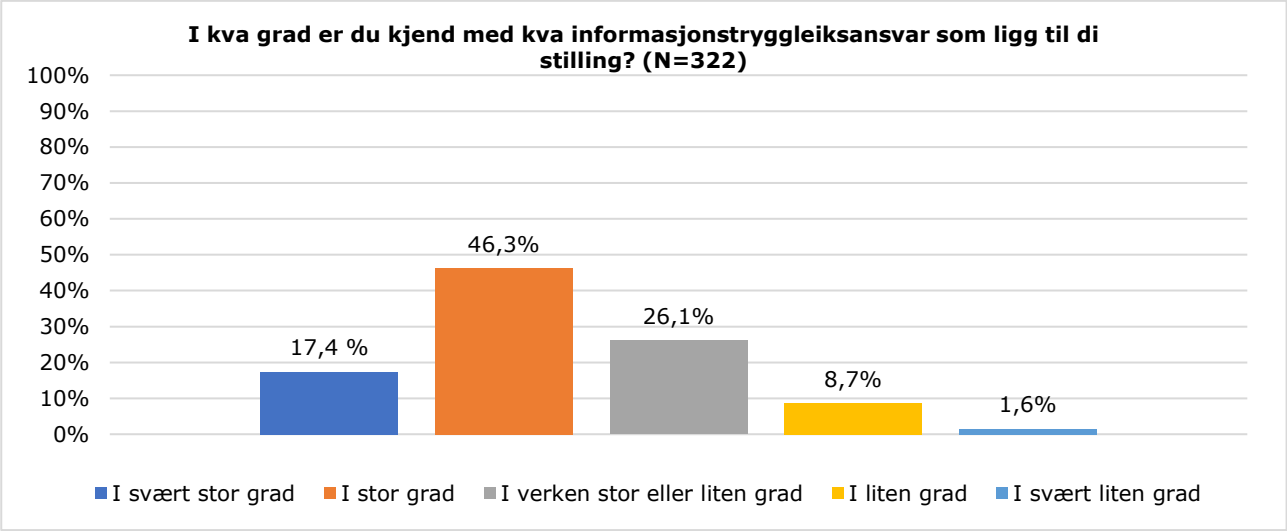


Respondentane i spørjeundersøkinga blei spurde om *dei er kjende med kva ansvar og oppgåver som ligg til deira stilling med omsyn til informasjonstryggleiken i kommunen*. Som det går fram av figur 9 svara totalt 63,7 % at dei anten «i svært stor grad» (17,4 %) eller «i stor grad» (46,3 %) er kjende med eige

[54] N=194
[55] N=226. 23,5 % svara «i svært stor grad», 41,2 % svara «i stor grad», 8,4 % «i liten grad», 1,3 % svara «i svært liten grad».

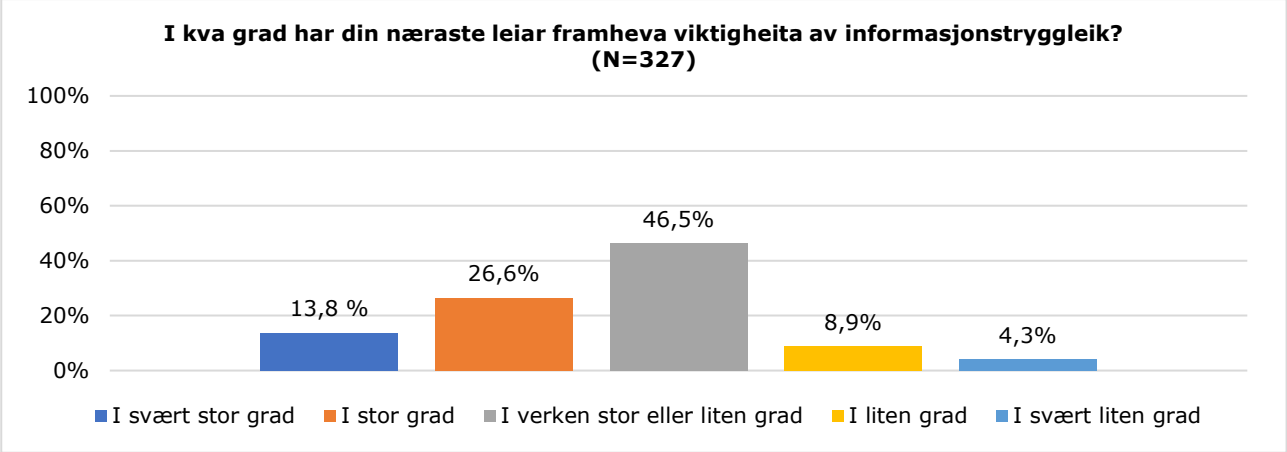
ansvar og eigne oppgåver knytt til informasjonstryggleik. Totalt 10,3 % av respondentane svara at dei anten «i liten grad» (8,7 %) eller «ikkje i det heile» (1,6 %) er kjende med kva ansvar og oppgåver dei har med omsyn til informasjonstryggleiken:

Figur 9: Kjennskap til eige ansvar og oppgåver knytt til informasjonstryggleik



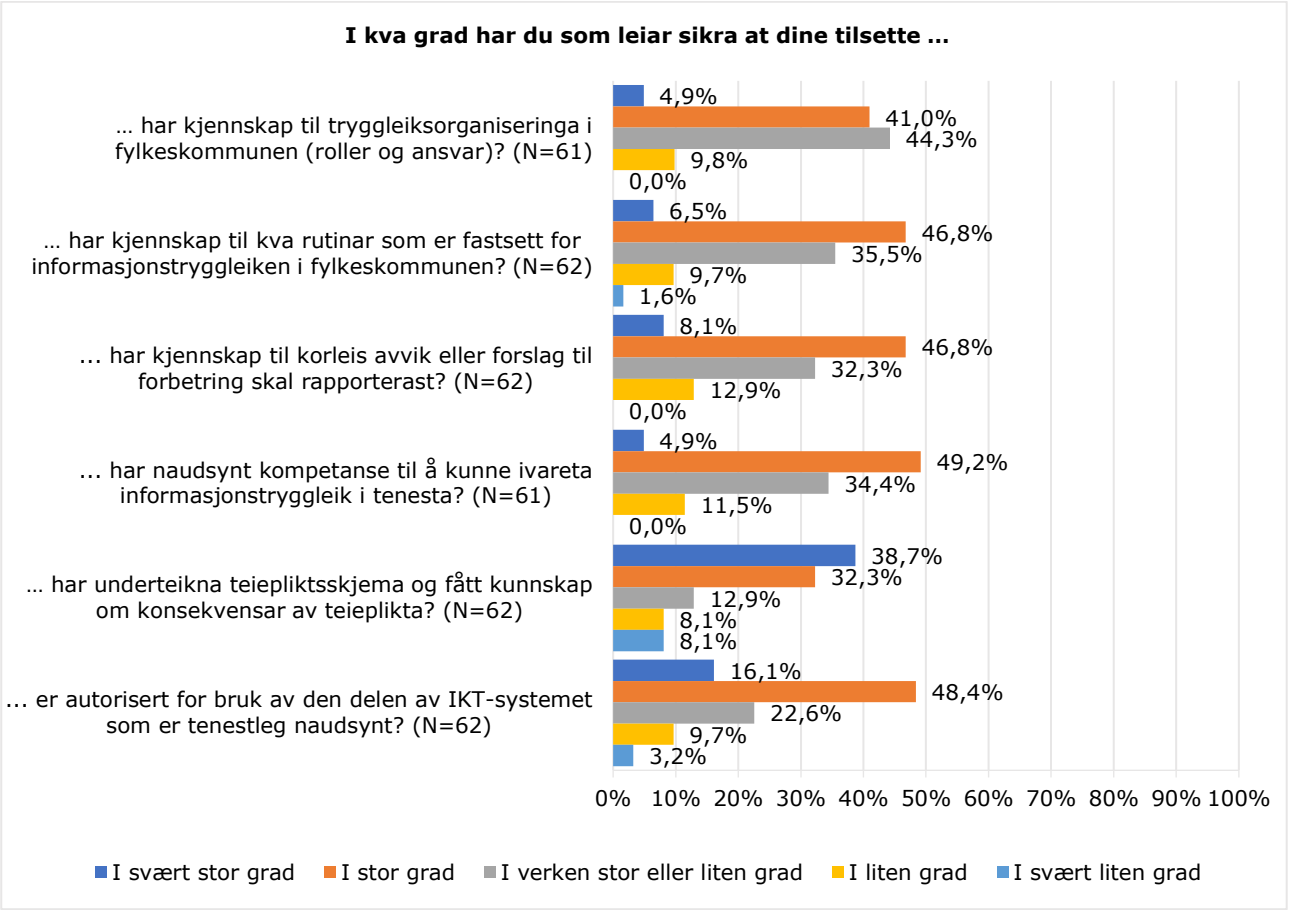
Svara på spørsmålet i *kva grad har din næraste leiar framheva viktigheita av informasjonstryggleik* blir presentert i figur 10 under. Som det går fram av figuren svara 46,5 % «i verken stor eller liten grad»:

Figur 10: Viktigheita av informasjonstryggleik



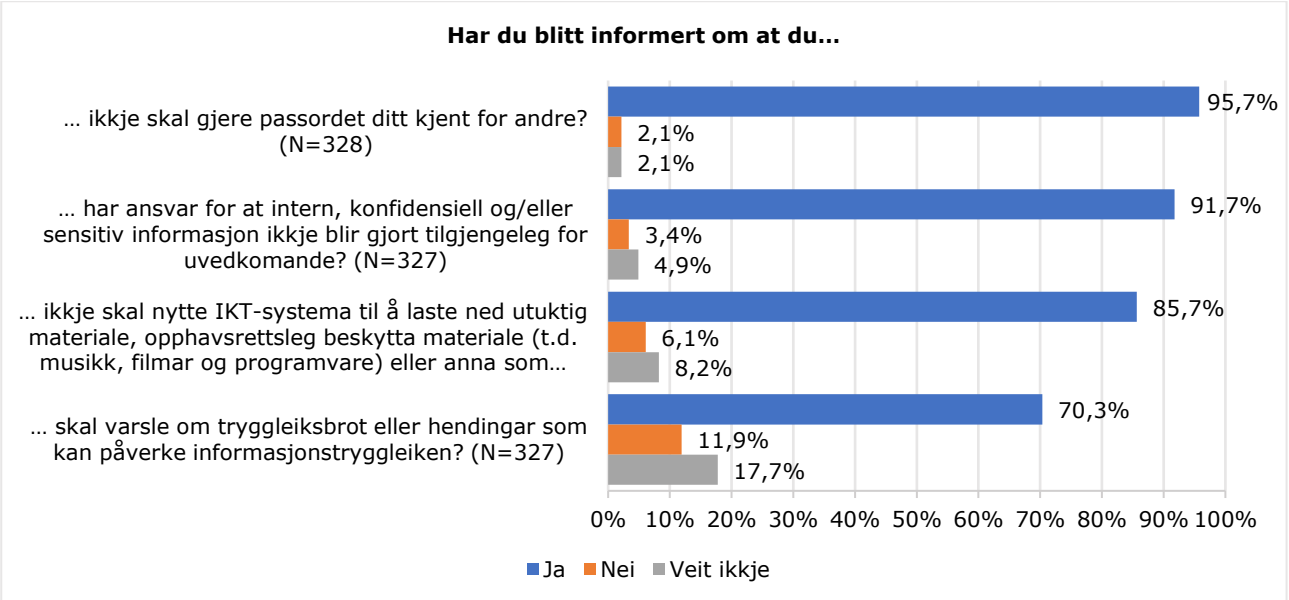
Dei som svara at dei har leiaransvar i fylkeskommunen ble stilt ei rekkje spørsmål knytt til korleis dei sikrar at deira tilsette følgjer opp fylkeskommunen sine retningslinjer for informasjonstryggleik. Som det går fram av figur 11 varierer det i kva grad leiarane har sikra at dei tilsette har fått opplæring og informasjon. Medan eit fleirtal svara at *dei tilsette har underskrive og kjenner til konsekvensane av teieplikta* (til saman 70,9 % svarar «i svært stor grad» og «i stor grad»), svara om 8,1 % «i svært liten grad» på dette spørsmålet. Vidare svara 11,5 % av leiarane at dei «i liten grad» *har sikra at dei tilsette har naudsynt kompetanse til å kunne ivareta informasjonstryggleik i tenesta.*

Figur 11: Opplæring av tilsette



Figur 12 viser respondentane som er tilsette i Vestland fylkeskommune sine svar på fem spørsmål i kva grad dei har blitt informert om ulike punkt som gjeld informasjonstryggleik. Svara indikerer at dei fleste har fått informasjon om informasjonstryggleik *som at passord ikkje skal gjerast kjent for andre* (95,7 %). Samtidig viser figuren at 11,9 % svara «nei» på spørsmål om *dei har blitt informert om at dei skal varsle om tryggleiksbrot eller hendingar som kan påverke informasjonstryggleiken.* 17,7 % svara «veit ikkje» på same spørsmål.

Figur 12: Opplæring i informasjonstryggleik Vestland fylkeskommune



Respondentane blei vidare spurde om dei *veit kven dei skal kontakte dersom dei har spørsmål knytt til informasjonstryggleik, handsaming av personopplysningar og/eller handsaming av fortruleg informasjon*. Her svara om lag halvparten «ja» (50,3 %) og halvparten «nei» (49,7 %).[56] Av dei 147 som svarte på oppfølgingsspørsmålet om kven dei skal kontakte, peikar eit fleirtal på nærmaste leiar som personen dei ville kontakta. Personvernombodet blir elles nemnd av fleire, noko som òg gjeld IT-avdelinga og HR-seksjonen.[57] Andre alternativ som blir nemnd er IKT-sikkerheitsrådgjevar, juristar på eiga avdeling og personvernrådgjevar.

Respondentane i spørjeundersøkinga fekk også spørsmål om dei er kjend med kva rutinar som gjeld for å melde avvik knytt til informasjonstryggleik. På dette spørsmålet svara 35,3 % av respondentane «ja» og 64,7 % av respondentane «nei».[58]

7.4.2 Vurdering

Vestland fylkeskommune har i nokon grad etablert prosedyrar og instruksar som legg til rette for at tilsette skal tileigne seg kunnskap og kompetanse knytt til informasjonstryggleik. Undersøkinga viser at denne dokumentasjonen nyleg er gjort tilgjengeleg for dei tilsette, og at ikkje alle tilsette er kjende med innhaldet.

T.d. viser undersøkinga at sjølv om majoriteten av respondentane handsamar eller kjem i kontakt med personopplysningar, sensitive personopplysningar eller anna fortruleg informasjon i arbeidskvardagen, svarar mellom 18 % og 22 % at dei ikkje veit i kva grad fylkeskommunen og/eller eininga dei jobbar i har tilfredsstillande skriftlege retningslinjer for handsaming av personopplysningar, sensitive person-opplysningar og anna fortruleg informasjon. Vidare svarar relativt mange av respondentane i spørjeundersøkinga at dei ikkje har (11,9 %) eller ikkje veit om det har (17,7 %) blitt informert om at dei skal varsle tryggleiksbrot og hendingar som kan påverke informasjonstryggleiken, og 64,7 % svara at dei ikkje er kjende med gjeldande rutinar for å melde avvik.

Revisjonen er merksam på at fylkeskommunen er i prosess med å ferdiggjere sitt styringssystem for informasjonstryggleik, og vidare at fylkeskommunen er open på at dei so langt ikkje har blitt gitt systematisk opplæring i informasjonstryggleik til dei tilsette (jf. seksjon 7.3). Likevel er det revisjonen si vurdering at fylkeskommunen ikkje i tilstrekkeleg grad har sørga for tilfredsstillande opplæring av dei tilsette, og at dette medfører ein risiko for brot på regelverk og anbefalingar på området grunna manglande kompetanse blant dei tilsette.

7.5 Etterleving av retningslinjer og rutinar for informasjonstryggleik

7.5.1 Datagrunnlag

I intervju blir det gjennomgåande vist til at informasjonstryggleikspraksisen blant dei tilsette i Vestland fylkeskommune er antatt å vere ganske svak. Dette blir forklart dels med at styringssystemet ikkje er ferdig utarbeidd og organisasjonen difor manglar mykje retningslinjer og rutinar for informasjonstryggleik. I tillegg blir det vist til at fylkeskommunen ikkje systematisk har gjennomført kompetansehevingstiltak på området. Samla fører dette til ei forventning blant fleire av dei intervjua om at dei tilsette ikkje er sett i stand til å praktisere god informasjonstryggleik. Det blir òg peika på at arbeidet med informasjonstryggleik nok er relativt ukjend for store delar av organisasjonen.

Som nemnd i kapittel 2 og andre plasser i rapporten, blir det også i denne samanheng vist til at organisasjonen er relativt ny, og at COVID-19-pandemien har gjort det ekstra utfordrande å både ferdigstille styringssystemet for informasjonstryggleik, og å få bygga ein organisasjon med ein god tryggleikskultur.

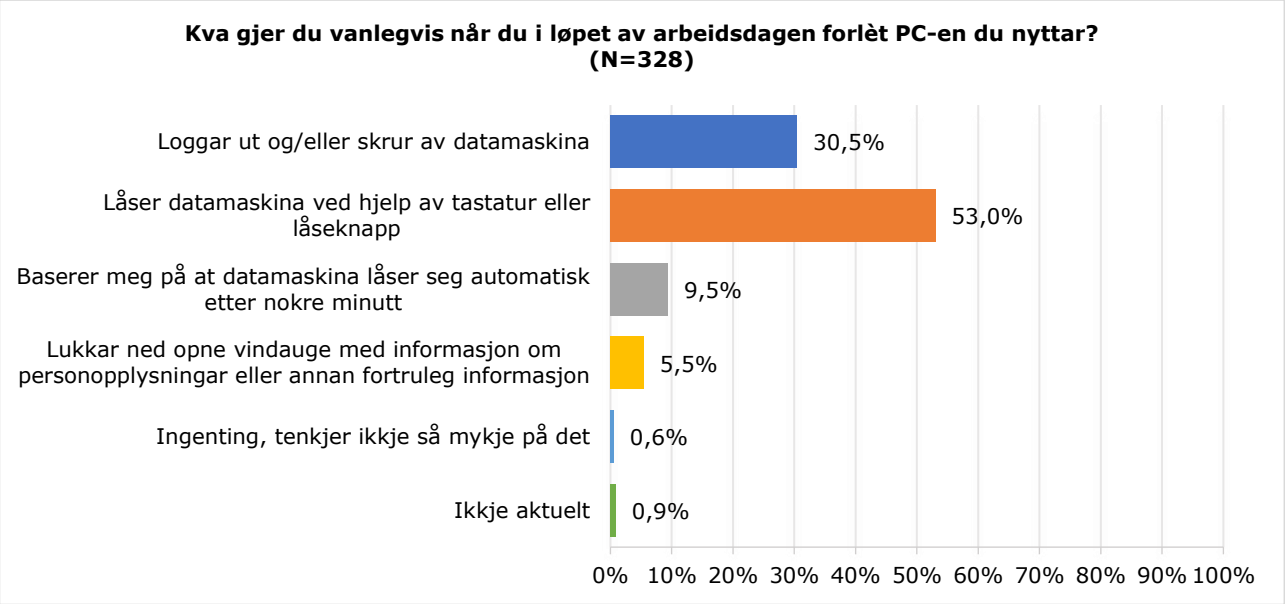
Det blir samtidig understreka at COVID-19-situasjonen har gjort at Vestland fylkeskommune har gjort store framsteg knytt til digital kommunikasjon på kort tid, framsteg som det i ein normalsituasjon ville tatt fleire år å oppnå; til dømes har det blitt gjennomført digitale fylkestingsete med om lag 80 deltakarar, og tilsette har hurtig tatt i bruk fleire digitale kommunikasjonsverktøy.

For å kartleggje etterlevinga av fylkeskommunen sine retningslinjer og rutinar på området, fekk respondentane i spørjeundersøkinga ei rekkje spørsmål knytt til deira eigen og andre sin informasjonstryggleikspraksis.

[56] N=328
[57] Nokre oppgjer namn på personar tilsett ved desse avdelingane, andre skriv berre namnet på seksjon/eining
[58] N=326

Respondentane blei t.d. i spørjeundersøkinga spurde om kvardagsrutinar når dei forlèt PC-en dei nyttar. Svara er presentert i figur 13:

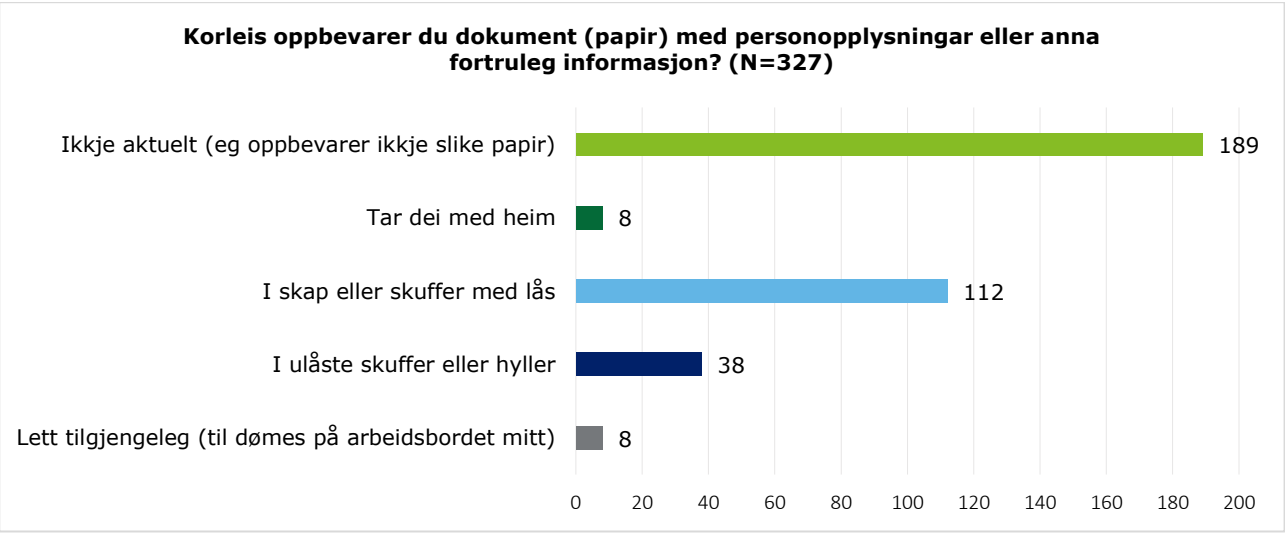
Figur 13 Kvardagsrutinar når tilsette forlèt PC-en



Respondentane blei også spurde om *dei nokon gong har lånt ut brukarnamn og passord til andre*. 86,8 % svara «nei», 11,4 % svara «ja, men berre til IKT-avdelinga eller tilsvarande» og 1,8 % svara «ja». Totalt har altså 13,2 % av respondentane delt passordet sitt med andre. I samband med verifiseringa av rapporten, opplyser fylkeskommunen at om ein tilsett delar passord med IT-tenesta, er det vanleg rutine at IT-tenesta ber brukaren om å endre passordet sitt etterpå.

På spørsmål om eigen praksis for å oppbevare papirdokument med personopplysningar eller anna fortruleg informasjon på, svara 38 av respondentane «i ulåste skuffer eller hyller», 8 svarar «lett tilgjengeleg (til dømes på arbeidsbordet mitt)». 3 av respondentane svara at dei tar med dokument med fortruleg informasjon heim (figur 14).[59]

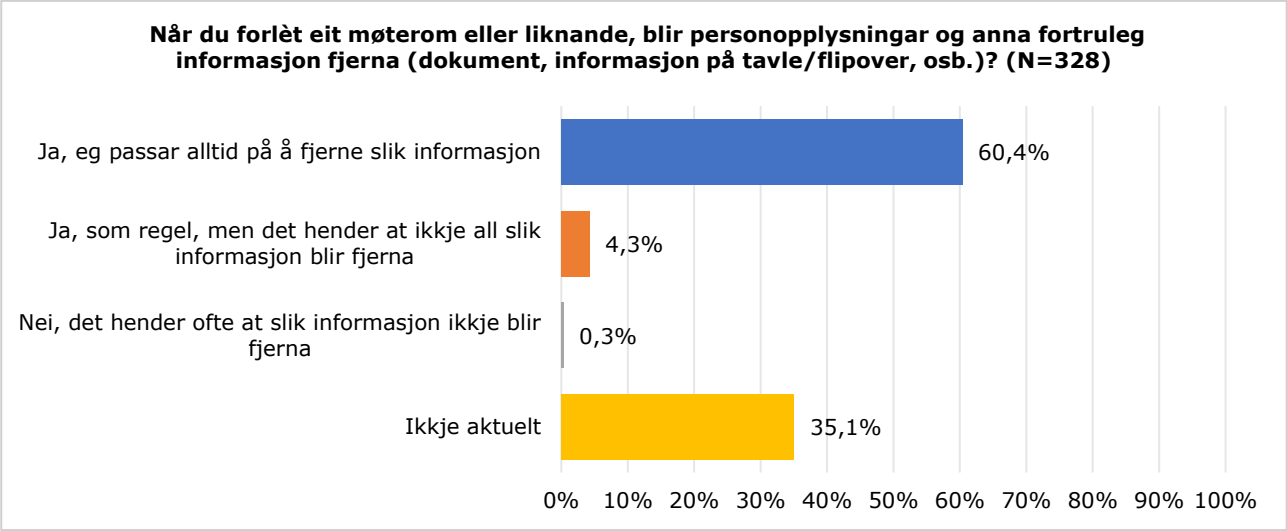
Figur 14: Oppbevaring av dokument



[59] Respondentane hadde høve til å velje meir enn eit svaralternativ på dette spørsmålet, og svara er difor ikkje prosentuert.

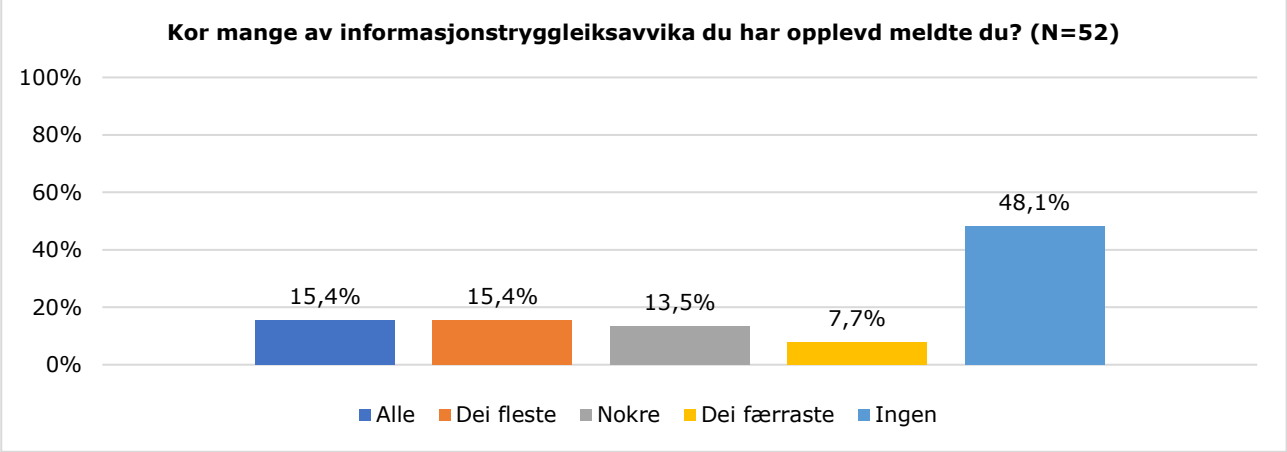
Respondentane fekk vidare spørsmål om dei fjernar fortruleg informasjon frå møterom når dei forlèt det. Som vist i figur 15 svara 4,3 % at dette som regel blir gjort, men at det hender at ikkje all slik informasjon blir fjerna, men 60,4 % oppgjer at dei alltid fjernar slik informasjon frå møterom.

Figur 15: Fjerning av fortruleg informasjon frå møterom



På spørsmål om *dei har opplevd eit eller fleire avvik knytt til informasjonstryggleik* svara 15,9 % av respondentane «ja».[60] Desse fekk oppfølgingsspørsmål om kor mange av informasjonstryggleiksavvika dei meldte vidare. Som det går fram i figur 16 svara 48,1 % av respondentane at dei ikkje meldte nokre av dei observerte avvika, medan totalt 21 % svara at dei meldte «nokre» (13,5 %) eller «dei færraste» (7,7 %).

Figur 16: Meldte informasjonstryggleiksavvik

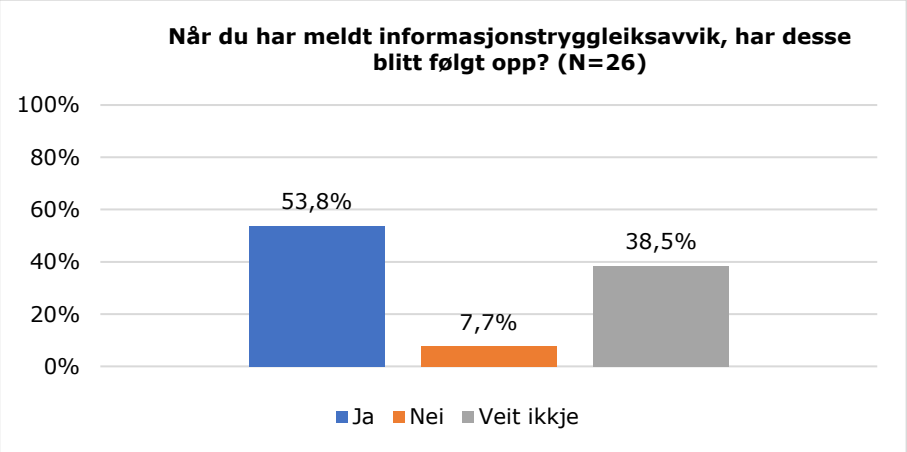


Respondentane som svara at dei meldte «ingen», «dei færraste», «nokre» eller «dei fleste» informasjonstryggleiksavvika dei hadde opplevd, fekk eit oppfølgingsspørsmål der dei blei bedne om å forklare årsaka til at dei ikkje melder alle avvik. Av dei 33 som svarte på dette spørsmålet var årsakene mellom anna at avviket har blitt retta opp direkte med den det gjeld (til dømes med ulåst PC blir det sagt ifrå om dette til eigar av PC-en), at ein ikkje veit kor eller korleis ein skal melde avvik og at ein vurderte grad av avvik som lite alvorleg.

Respondentane som svara at dei har meldt «alle», «dei fleste», «nokre» eller «dei færraste» informasjonstryggleiksavvik fekk spørsmål om dei meldte avvika blei følgt opp. Svara går fram i figur 17:

[60] N=327. 54,5 % svara «nei» og 29,7 % svara «veit ikkje».

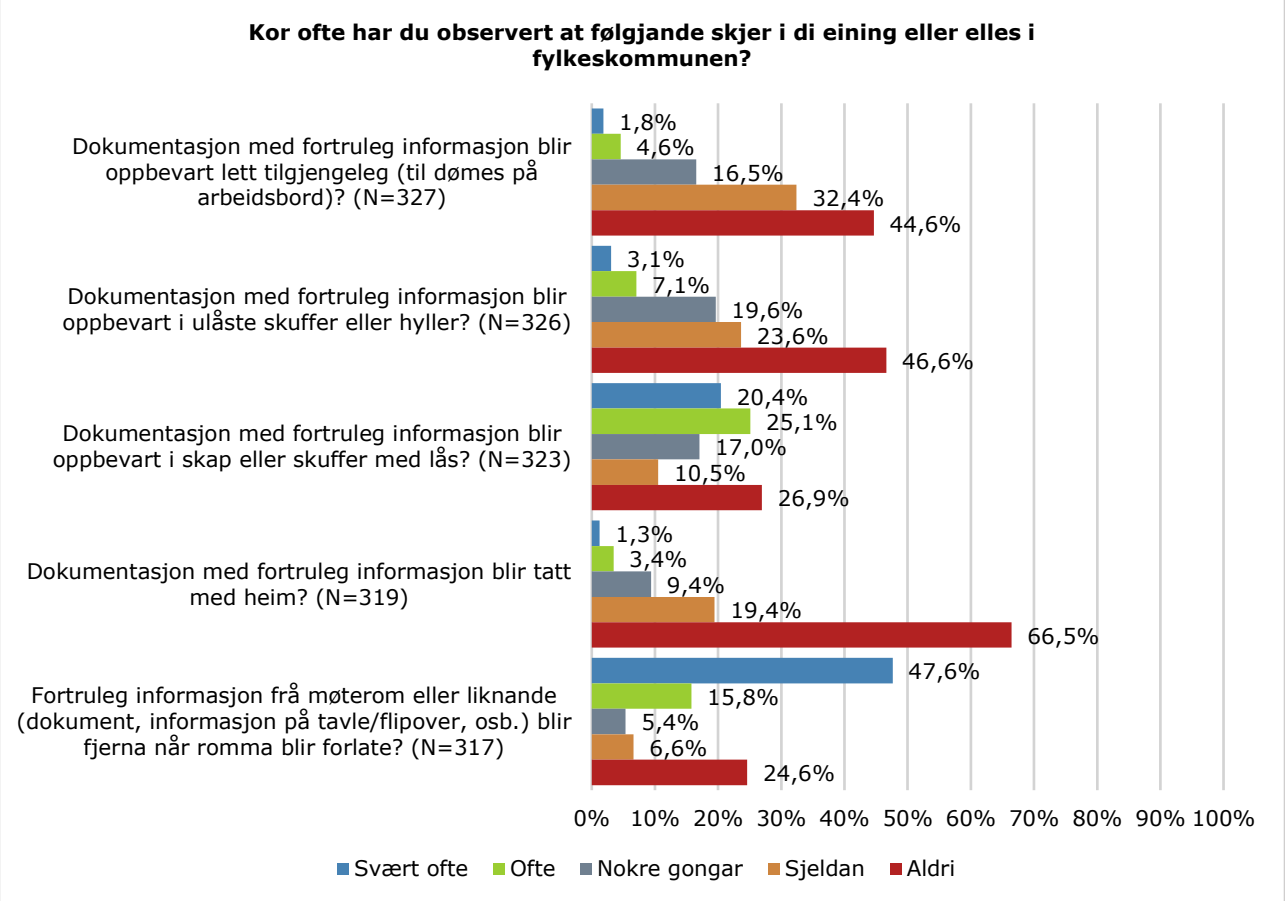
Figur 17: Oppfølging av meldte avvik



Andre sin informasjonstryggleikspraksis

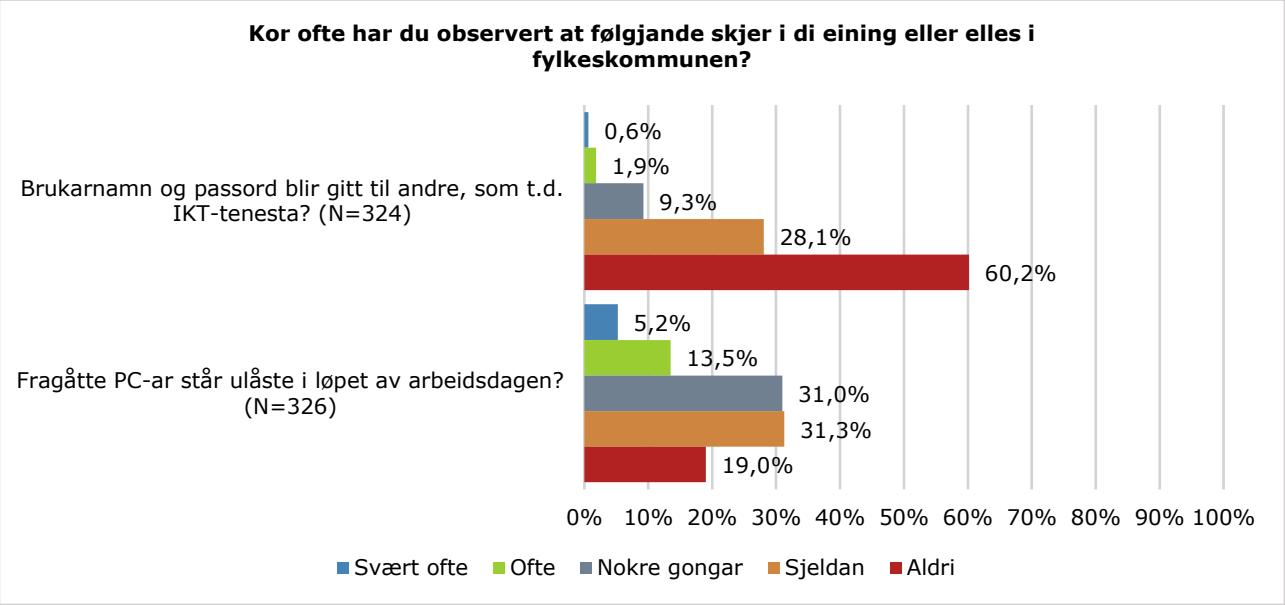
Respondentane blei i spørjeundersøkinga bedne om å svare på ein del spørsmål knytt til kollegaar sin informasjonstryggleikspraksis. Mellom anna blei dei spurde om kor ofte dei *har observert at fortruleg informasjon frå møterom eller liknande (dokument, informasjon på tavle/flippover, osb.) blir fjerna når romma blir forlatne* Resultata (sjå figur 18) viser mellom anna at 24,6 % svarar «aldri» på spørsmål om fortruleg informasjon frå møterom eller liknande blir fjerna når romma blir forlatne.

Figur 18: Informasjonstryggleikspraksis – dokument



Respondentane blei òg spurde om kollegaar sin informasjonstryggleikspraksis knytt til deling av passord og om fragåtte PC-ar står ulåste i løpet av arbeidsdagen (sjå figur 19). Nesten 40 % svara at dei har observert deling av brukarnamn og passord, og 81 % har observert at fragåtte PC-ar står ulåste i løpet av arbeidsdagen.

Figur 19: Informasjonstryggleikspraksis – passord og PC



7.5.2 Vurdering

Undersøkinga viser at retningslinjer og rutinar for informasjonstryggleik i liten grad blir etterlevd i Vestland fylkeskommune. Rett nok tyder svara i spørjeundersøkinga på at dei fleste respondentane sjølve praktiserer god informasjonstryggleik når dei forlét PC-ane sine, og vidare at problemstillingar knytt til fortrulegheit og personvern når det gjeld papirdokument og møterom verkar å vere uaktuelle for dei fleste respondentane. Men sjølv på desse områda er det fleire som ikkje har ein god praksis; 15 % svarar at dei ikkje loggar ut eller låsar PC-en sin når dei forlét denne, og 81 % har observert dette hos andre. Vidare svarar fleire av respondentane at dei sjølve tar med papirdokument med fortruleg informasjon eller personopplysningar heim, og at slike dokument blir oppbevart både ulåst og lett tilgjengeleg. Over halvparten av respondentane har vidare observert at andre har oppbevart slike dokument lett tilgjengeleg og i ulåste skuffer eller hyller, og nesten 40 % har observert at slike dokument har blitt tatt med heim.

Vidare kjem det fram at 13,2 % av respondentane sjølve har delt brukarnamn og passord med andre, og nesten 40 % har observert at dette har skjedd blant kollegaar. Revisjonen er merksam på at det i Vestland fylkeskommune er vanleg rutine at tilsette som delar passord med IT-tenesta blir bedne om å endre passordet sitt etterpå. Revisjonen vil likevel understreke at det å dele passord med andre ikkje er i samsvar med grunnleggjande prinsipp for informasjonstryggleik eller fylkeskommunen sine eigne retningslinjer, og at dette også gjeld dersom det er IT-tenesta ein deler passordet med.

I tillegg kjem det fram at berre 15,4 % av dei som har opplevd informasjonstryggleiksavvik, har meldt alle desse, og at 48,1 % av dei som har opplevd slike avvik ikkje har meldt nokon av dei. Revisjonen vil i den samanheng peike på at manglande avviksmeldingar aukar risikoen for at svakheiter i system og organisasjon ikkje blir retta, og vidare at manglande oppfølging av innmeldte avvik kan dempe motivasjonen for å melde avvik, og slik auke risikoen for at nye avvik ikkje blir meldt.

Basert på funna frå undersøkinga, er det revisjonen si vurdering at dei tilsette i Vestland fylkeskommune i liten grad etterlever retningslinjer og rutinar for informasjonstryggleik. Dette gjev auka risiko for informasjonstryggleiksbrot, og revisjonen meiner fylkeskommunen må gjere tiltak for å sikre etterleving av retningslinjer og rutinar for informasjonstryggleik.

8. Konklusjon og tilrådingar

Denne forvaltningsrevisjonen har undersøkt og vurdert om Vestland fylkeskommune har tilfredsstillande system og rutinar for informasjonstryggleik, om etablerte standardar og gjeldande lovar og reglar blir følgt innanfor dette området, korleis fylkeskommunen praktiserer informasjonstryggleik med omsyn til konfidensialitet og tilgangsstyring, i kva grad fylkeskommunen etterlever sentrale krav i ny personvernlovgjeving, og kva kompetanse dei tilsette har på området.

Styringssystem for informasjonstryggleik

Undersøkinga finn at Vestland fylkeskommune framleis er i prosess med å få etablert eit styringssystem for informasjonstryggleik. Sjølv om dei styrande dokumenta i styringssystemet i hovudsak er ferdige og tilgjengelege for dei tilsette, står det att ein del arbeid før systemet er ferdig, og fylkeskommunen opplyser at det også vil ta tid før eit ferdig system er implementert i organisasjonen.

Det at styringssystemet for informasjonstryggleik ikkje er ferdig og ikkje er implementert i organisasjonen har fleire konsekvensar. Mellom anna finn revisjonen at dei formelle ansvarsforholda knytt til informasjonstryggleik ikkje blir praktisert som føresett, og vidare at sjølv dei delane av styringssystemet som er ferdig, i liten grad er kjend i organisasjonen, og følgjeleg også i liten grad blir følgt.

Både etableringa av Vestland fylkeskommune og COVID-19-pandemien blir vist til som forklaringar for kvifor styringssystemet ikkje er ferdig utarbeidd og ikkje er ferdig implementert i organisasjonen. Likevel vil revisjonen understreke viktigheita av å ferdigstille og implementere styringssystemet for informasjonstryggleik, då dette er ein føresetnad for at fylkeskommunen kan etablere ein god informasjonstryggleikspraksis.

Sikring av konfidensialitet

Vestland fylkeskommune har gjort både organisatoriske og tekniske tiltak for **sikring av konfidensialitet**. Mellom anna har fylkeskommunen langt på veg sett i verk tilstrekkelege tiltak for å sikre at konfidensiell informasjon kan bli *lagra* trygt. Vidare er det stilt krav om at konfidensiell informasjon som *ikkje* blir lagra trygt, skal krypterast, med det er ikkje utarbeidd rutinar eller prosedyrar for korleis slik kryptering skal skje. Følgjeleg er det risiko for at konfidensielle opplysningar i Vestland fylkeskommune som ikkje blir lagra trygt, heller ikkje blir kryptert. Fylkeskommune har vidare fleire retningslinjer og rutinar som er eigna til å bidra til å hindre uautorisert innsyn i konfidensielle opplysningar. Undersøkinga tyder på at desse ikkje alltid blir etterlevd, og det er følgjeleg revisjonen si vurdering at fylkeskommunen ikkje i tilstrekkeleg grad hindrar uautorisert innsyn i konfidensielle opplysningar.

Tilgangsstyring

Vestland fylkeskommune har etablert rutinar for tilgangsstyring og for å **hindre uautorisert tilgang til informasjonssystema**. Fylkeskommunen har òg ein praksis på desse områda som langt på veg er automatisert, og som slik bidreg til å hindre uautorisert tilgang til mange av informasjonssystema. Likevel avdekker undersøkinga manglar i både rutinar, system og praksis knytt til tilgangsstyringa; mellom anna krev tilgangsstyringa i nokre av informasjonssystema manuelle operasjonar, noko som aukar risikoen for at tilsette får feile tilgangar. Vidare viser undersøkinga at ikkje alle tildelte tilgangar til informasjonssystema jamleg blir gjennomgått og vurdert. I tillegg kjem det fram at ikkje alle brukte tilgangar i informasjons-systema blir loggført. Manglande loggføring av brukte tilgangar gjer at det ikkje er mogleg å avdekke eventuell uautorisert bruk av systema. Samla er det revisjonen si vurdering at Vestland fylkeskommune ikkje fullt ut har system, rutinar og praksis som hindrar uautorisert tilgang til informasjonssystema.

Etterleving av sentrale krav i personvernlovgjevinga

Vestland fylkeskommune tilsette eit **personvernombod** i 50 % 17. august 2020, med tilhøyrande ansvar og oppgåver. Revisjonen har ikkje avdekt noko som indikerer at mandatet til personvernombodet i Vestland fylkeskommune ikkje oppfyller krava i artikkel 39 i personvernforordringa.

Fylkeskommune har delvis rutinar og prosedyrar for føring av **protokoll over behandlingar av personopplysningar**, og har begynt arbeidet med å føre slik protokoll. Dette arbeidet var på revisjonstidspunktet ikkje ferdig. Fylkeskommunen bryt slik med kravet i personvernforordninga artikkel 30 nr. 1, om å føre protokoll over behandlingsaktivitetar av personopplysningar.

Vestland fylkeskommune har vidare etablert skriftlege rutinar for inngåing av **databehandlaravtalar**, men har ikkje fullstendig oversikt over kva databehandlaravtalar som er inngått. Det er pågåande arbeid med å etablere slik oversikt. På revisjonstidspunktet meiner revisjonen det er høg risiko for at fylkeskommunen ikkje oppfyller kravet i personvernforordninga artikkel 28 nr. 3.

Vestland fylkeskommune har etablert rutinar for gjennomføring av **risikovurderingar knytt til behandling av personopplysningar og personvernkonsensvurderingar (DPIA)**. Undersøkinga viser òg at det har blitt gjennomført nokre slike risikovurderingar, men ikkje for alle behandlingar av personopplysningar. Fylkeskommunen bryt slik med personvernforordninga artikkel 32 nr. 1.

Kompetanse om informasjonstryggleik

Vestland fylkeskommune har gjennom dei delane av styringssystemet for informasjonstryggleik som er ferdig, plassert ansvar og oppgåver knytt til **opplæring** innanfor informasjonstryggleik. Vidare skal alle tilsette i Vestland fylkeskommune vere informert om grunnleggjande informasjonstryggleikskrav gjennom internt regelverk. Fylkeskommunen er open på at opplæring av tilsette ikkje har blitt prioritert før organisasjonen har gjort ferdig nødvendig dokumentasjon i styringssystemet, og at det difor ikkje har blitt gitt systematisk opplæring på dette området. Det er heller ikkje lagt konkrete planar for korleis slik opplæring skal bli gitt. Resultatet frå spørjeundersøkinga understrekar dette; relativt mange av respondentane **ønskjer meir opplæring** på området, mange av dei er ikkje godt kjend med dei rutinane og retningslinjene som finst for informasjonstryggleik i Vestland fylkeskommune, og at mange praktiserer heller ikkje god informasjonstryggleik. Det er følgjeleg revisjonen si vurdering at Vestland fylkeskommune ikkje oppfyller krav og anbefalingar knytt til å sikre tilstrekkeleg informasjonstryggleikskompetanse blant dei tilsette gjennom opplæringstiltak, og at dei tilsette i Vestland fylkeskommune ikkje alltid etterlever retningslinjer og rutinar for informasjonstryggleik. Dette gjev auka risiko for informasjonstryggleiksbrot.

Tilrådingar

Basert på funna i undersøkinga, tilrår revisjonen at Vestland fylkeskommune gjennomfører tiltak for å sikre følgjande:

1. at fylkeskommunen sitt styringssystem blir gjort ferdig og implementert i organisasjonen, og som del av dette sikre at:
   a) ansvarsforhold knytt til informasjonstryggleik blir gjort kjend og etterlevd av dei tilsette
   b) rutinar for informasjonstryggleik blir gjort ferdige, kjende og blir etterlevd av dei tilsette
   c) det blir gjennomført tilstrekkeleg kontroll og etterprøving av informasjonstryggleiken
2. at ansvar og rutinar for å hindre uautorisert innsyn i konfidensielle opplysningar er utfyllande, tydelege og blir etterlevd, og som del av dette gjer tiltak for at tilsette:
   a) praktiserer trygg bruk av e-post, t.d. gjennom nettfiskeforsøk
   b) nyttar sikker sone ved lagring av konfidensielle opplysningar
   c) krypterer konfidensielle opplysningar som ikkje er lagra i sikker sone
3. at ansvar og rutinar for å hindre uautorisert tilgang til informasjonssystema er utfyllande, tydelege og blir etterlevd, og som del av dette gjer tiltak for å:
   a) sikre at tilsette har nødvendige tilgangar
   b) sikre at tilsette ikkje har tilgangar utan at det er tenestleg behov
4. at krava i personvernforordninga blir etterlevde, og som del av dette:
   a) føre protokoll over alle behandlingar av personopplysningar
   b) signere databehandlaravtalar med alle kommunen sine databehandlarar
   c) gjennomføre risikovurderingar knytt til behandlingar av personopplysningar
   d) gjennomføre vurdering av personvernkonsekvensar ved behandlingar av personopplysningar med høg risiko
5. at systemeigarar og andre med ansvar knytt til informasjonstryggleik og personvern mottek tilstrekkeleg opplæring
6. at det blir utarbeidd tilstrekkeleg med informasjon om informasjonstryggleik til dei tilsette, og sikre at dei tilsette får den naudsynte opplæringa for å kunne ivareta informasjonstryggleiken på ein tilfredsstillande måte.

Vedlegg 1: Høyringsuttale

Vestland fylkeskommune

Strategisk utvikling og digitalisering
SUD - Stab

Vår referanse 2020/75692-4
Dato 11.11.2020

Deloitte AS
Postboks 6013 Postterminalen
5892 Bergen

v/ Frode Løvlie

Ikkje offentleg: jf. offl. § 14 1. ledd, interne dokument

Svar - Forvaltningsrevisjon Vestland fylkeskommune - informasjonstryggleik

Fylkesrådmannen viser til utkast revisjonsrapport «Forvaltningsrevisjon Vestland fylkeskommune - informasjonstryggleik», motteke i e-post dagsett 30.10.2020.

I dette brevet fylgjer fylkesrådmannen sin høyringsuttale til rapporten.

Generelle merknader
Dei føreslegne tiltaka gir ein god plan for vidare arbeid med informasjonstryggleik i fylkeskommunen. Nokre av tiltaka er allereie under arbeid, nokre er enkle å gjennomføre. Andre er særs arbeidskrevjande. Utgangspunktet for rapporten er Vestland fylkeskommune, heretter VLFK, sitt styringssystem for informasjonssikkerheit. Ved oppstart av forvaltningsrevisjonen, og før intervju vart gjennomført, informerte vi revisor om at styringssystem for informasjonssikkerheit ikkje var ferdig. Dette som følgje av etablering av den nye fylkeskommunen 1.januar 2020. Resultata i rapporten er prega av dette, då dei forskjellige kapitla (styringssystem for informasjonstryggleik, konfidensialitet, tilgangsstyring, personvern, kompetanse om informasjonstryggleik) er underlagt styringssystem for informasjonssikkerheit. IKT-sikkerheitsrådgjevar starta i stillinga 15 april, ein månad før revisjonen vart bestilt. Personvernombod starta 17. august. Fram til denne dato har vi hatt mellombelse personvernombod og personvernrådgjevar sidan oppstarten av VLFK.

Spesifikke merknader

Rutinar og ansvarsforhold knytt til informasjonstryggleik:
Praksis er ikkje etablert i organisasjonen endå, fordi dokumenta har vorte ferdiggjort under revisjonen og ikkje er sendt ut til organisasjonen. Difor er det heller ikkje noko å kontrollere eller etterprøve.

Etterleving av sentrale krav i personvernlovgjevinga:
Å gå gjennom databehandlaravtale, personvern protokoll og PIA-ROS vurdering for alle system i VLFK er lagt inn i årshjulet til IKT-sikkerheitsrådgjevar, personvernombod og personvernrådgjevar. Vi
må utarbeide en fullstendig oversikt og dette vil ta tid. Risikoregister vart ferdig 30. oktober 2020.

Merknader til føreslegne tiltak
Fylkesrådmannen meiner at føreslegne tiltak generelt sett er gode og er samd i at dei er naudsynte i
arbeidet med informasjonstryggleik i fylkeskommunen. Fleire av tiltaka vert allereie arbeida kontinuerleg med.

Tiltak 1 (a-c):
Fylkesrådmannen er samd i tiltaka og dette er allereie under arbeid. Det er ein omfattande prosess,
med å utarbeide all dokumentasjon og få denne formidla ut til tilsette for så å bli effektivt implementert i arbeidskvardagen. Når styringssystem for informasjonssikkerheit er kome godt på plass, vil det gje meining å gjere kontroll og etterprøving. Vi vil leggje opp til rutinar for kontroll og

Telefon 05557 | E-post post@vlfk.no | Heimeside www.vestlandfylke.no | EHF-Fakturaadr. 821311632 | Organisasjonsnr. 821 311 632

etterprøving.

Tiltak 2 (a-c):
Fylkesrådmannen er samd i tiltaka. Rutinar for lagring og handsaming av konfidensielle opplysingar/personopplysingar er under utarbeiding.

Tiltak 3 (a-b):
Fylkesrådmannen er samd og anerkjenner behovet for betre tilgangskontroll. Dette er ein innsats som vil gå på tvers av avdelingar og krevje ressursar frå alle avdelingar som har eigne fagsystem.

Tiltak 4: (a-d):
Fylkesrådmannen er samd i tiltaket, men vil peike på at det er arbeidskrevjande og vil ta tid. IKT-sikkerheitsrådgjevar skal også få på plass styringssystem for informasjonssikkerheit.

Tiltak 5:
Ingen merknad

Tiltak 6:
Fylkesrådmannen er samd i tiltaket og vil starte med e-læring i november. I tillegg har IKT-sikkerheitsrådgjevar oppretta eit intranettområde som er oppdatert, med gratis kurs og artiklar om forskjellige emne. Det er også oppretta e-post adresse for sikkerheit (sikkerheit@vlfk.no) og personvernombod (personvernombod@vlfk.no)

Fyrste prioritet for VLFK er å få ferdig nødvendig dokumentasjon og få dette sendt ut til dei tilsette, saman med opplæring av tilsette og oppbygging av sikkerheit- og personvernorientert kultur.

Med helsing

Rune Haugsdal
fylkesrådmann

Paal Fosdal
fylkesdirektør

Brevet er elektronisk godkjent og har difor inga handskriven underskrift

Mottakarliste
Frode Løvlie

Vedlegg 2: Revisjonskriterium

Informasjonstryggleik

Informasjonstryggleik handlar om trygging av informasjon med omsyn til *konfidensialitet*, *integritet* og *tilgjengelegheit*.

Å sørgje for *konfidensialitet* inneber å hindre ikkje-autorisert innsyn i informasjon som ikkje skal vere tilgjengeleg for alle; å sørgje for *integritet* inneber å hindre ikkje-autorisert endring og sletting av informasjon; å sørgje for *tilgjengelegheit* inneber å sikre tilgang til informasjon ved behov for tilgang.

Krav i lov og forskrift

Regelverket knytt til informasjonstryggleik omfattar mellom anna personopplysningslova.[61] Denne tredde i kraft 20. juli 2018, og gjennomfører EU si personvernforordning – kjend som GDPR[62] – i norsk lov.

Artikkel 4 i personvernforordninga definerer omgrepa brukt i forordninga i 26 punkt. Under er nokre relevante punkt presentert:

> 1) «personopplysninger» enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet,
>
> 2) «behandling» enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring
>
> …
>
> 7) «behandlingsansvarlig» en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes …
>
> 8) «databehandler» en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige
>
> …
>
> 12) «brudd på personopplysningssikkerheten» et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet

I fylkeskommunen er det fylkesrådmannen som er behandlingsansvarleg.[63] Databehandlarar er eventuelle tenesteleverandører til fylkeskommunen som behandlar personopplysningar, som til dømes leverandør av lønn- og personalsystem. Forordninga artikkel 28 nr. 3 stiller krav om at behandling av personopplysningar utført av ein databehandlar skal vere underlagt ein avtale med nærare spesifisert innhald (bokstav a til h).

Internkontroll og styringssystem for informasjonstryggleik

Artikkel 24 og 28 i forordninga omhandlar den behandlingsansvarlege og databehandlaren sitt ansvar for å etablere internkontroll; nr. 1 i artikkel 24 seier mellom anna at den behandlingsansvarlege skal «gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov», mens artikkel 28 nr. 1 stiller krav om at databehandlarar skal gi tilstrekkeleg med garantiar «for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordningen og vern av den registrertes rettigheter.»

---

[61] Lov om behandling av personopplysninger (personopplysningsloven)
[62] General Data Protection Regulation.
[63] Jf. *En veiledning om internkontroll og informasjonssikkerhet* (Datatilsynet 2009, s. 11).

Personvernforordninga artikkel 32 nr. 1 stiller vidare krav om informasjonstryggleik ved behandling av personopplysningar. Krava som stilles er at informasjonstryggleiken skal vere tilfredsstillande med omsyn til personopplysningane si konfidensialitet, integritet, tilgjengelegheit og robustheit gjennom at det blir sett i verk eigna tekniske og organisatoriske tiltak basert på risikovurderingar. Artikkelen inneheld føresegn som omhandlar kva risikovurderingane skal leggje vekt på.

I tillegg til føresegna i personvernforordninga knytt til internkontroll og informasjonstryggleik, er fylkeskommunen gjennom eForvaltningsforskrifta § 15 forplikta til å ha eit internkontrollsystem basert på anerkjende standardar for styringssystem for informasjonstryggleik:

> Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.
>
> Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.

Direktorat for forvaltning og IKT (Difi) er peika ut som ansvarleg for å gje tilrådingar knytt til kva styringssystem for informasjonstryggleik som bør nyttas. Difi tilrår at offentlege verksemder baserer seg på ISO/IEC 27001:2013, som er ein internasjonal standard for styringssystem for informasjonstryggleik.

Handsaming av personopplysningar

Personvernforordninga stiller krav om at fylkeskommunen skal informere registrerte personer om at den handsamar personopplysningar om dei, jf. artikkel 12-14. Artikkel 12 nr. 1 pålegg fylkeskommunen at slik informasjon skal vere «kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk.» Datatilsynet skriv i sitt rettleiingsmateriell at ein behandlingsansvarleg t.d. kan etterkome deler av informasjonskrava ved å ha ei personvernerklæring.

Forordninga stiller vidare nye og skjerpa krav til kva avvik som skal meldast til Datatilsynet. Hovudregelen slik denne går fram i artikkel 33 er at alle avvik som skuldast brot på personopplysningstryggleiken (utilsikta sletting, tap, endring, ulovleg spreiing av eller tilgang til personopplysningar som er overført, lagra eller på anna måte handsama, jf. artikkel 4 punkt 12), skal meldast til Datatilsynet innan 72 timar. Artikkel 33 nr. 3 stiller krav kva avviksmeldingane skal innehalde. Artikkel 34 stiller nærare krav om kva vilkår som må vere oppfylt for at fylkeskommunen *ikkje* skal melde i frå om personopplysningstryggleiksbrotet til den eller dei registrerte som avviket gjeld. Jf. artikkel 33 punkt 5, skal fylkeskommunen dokumentere alle avvik, og kva tiltak som er sett i verk.

Artikkel 30 nr. 1 i personvernforordninga stiller krav om at fylkeskommunen skal føre ein protokoll over behandlingsaktivitetane av personopplysingar som blir utført. Forordninga stiller nærare krav til innhaldet i denne protokollen, som t.d. namn og kontaktopplysning på den behandlingsansvarlege (bokstav a), formålet med behandlinga (bokstav b), ei skildring av kategoriane av registrerte og kategoriane av personopplysningar (bokstav c). Nr. 3 i artikkelen stiller krav om at protokollen skal vere skriftleg og nr. 4 seier at protokollen skal gjerast tilgjengeleg for Datatilsynet dersom dei ber om det.

Forordninga stiller i tillegg krav om at det i nokre situasjonar skal gjerast risikovurderingar av handsaminga av personopplysningar. I artikkel 35 nr. 1, står det at:

> Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for vernet av personopplysninger.

Dette er eit krav om at fylkeskommunen skal gjennomføre ei vurdering av personverkonsekvensane av handsaming av personopplysningar der slik handsaming medfører høg risiko for rettar og fridom for fysiske personar. Jf. artikkel 39 om personvernombodet sine oppgåver, skal vedkomande gi råd om vurdering av personvernkonsekvensar og kontrollere gjennomføringa av denne dersom fylkeskommunen ber om det.

Kompetanse

Som nemnd er fylkeskommunen gjennom eForvaltningsforskrifta § 15 forplikta til å ha ein internkontroll basert på anerkjende standardar for styringssystem for informasjonstryggleik. Departementet har peika ut direktorat for forvaltning og IKT (Difi) som ansvarleg for å gje tilrådingar knytt til kva styringssystem for informasjonstryggleik som bør nyttast, og Difi tilrår at offentlege verksemder baserer seg på ISO/IEC 27001:2013. Kapittel 7.2 i standarden seier at fylkeskommunen skal:

a) fastslå hvilken kompetanse som er nødvendig for personen(e) som utfører arbeid under organisasjonens styring, og som påvirker dens informasjonssikkerhetsprestasjon;
b) sikre at disse personene har kompetanse tilegnet gjennom passende utdanning, opplæring eller erfaring;
c) der det er relevant, treffe tiltak for å erverve nødvendig kompetanse og evaluere virkningen av tiltakene som er truffet; og
d) oppbevare relevant dokumentert informasjon som bevis på kompetanse.

I merknaden til punkt 7.2, står det at «Aktuelle tiltak kan for eksempel omfatte å sørge for opplæring, veiledning eller omplassering av nåværende ansatte eller innleie av eller kontraktinngåelse med kompetente personer.»

I Datatilsynet sin rettleiar *Internkontroll og informasjonssikkerhet*[64] omhandlar mellom anna oppfølging og opplæring. Her går det fram at målet med brukaropplæring er å syte for at brukarane er merksame på truslar mot personvernet og informasjonstryggleiken generelt, og at dei er gitt høve til å etterleve dette i sitt daglege arbeid. Opplæringa bør vere tilpassa dei ulike målgruppene sitt behov for opplæring og fordelast over tid. Brukarane bør få opplæring i rutinar, tryggleiksprosedyrar og riktig bruk av informasjonssystem for å redusere potensielle risikoar.

I tillegg til tilrådinga om opplæring av tilsette som følgjer av ISO-standarden, kan ein utleie eit krav om opplæring og kjennskap til system, rutinar og regelverk blant tilsette frå kommuneloven § 23 nr. 2, som seier at rådmannen skal «sørge for at administrasjonen drives i samsvar med lover, forskrifter og overordnede instrukser, og at den er gjenstand for betryggende kontroll.» Dette inneber at ein må ha eit system for internkontroll på plass for å sikre forsvarleg sakshandsaming. Eit sentralt tiltak i eitkvart internkontrollsystem vil vere at det er på plass tilstrekkeleg opplæring til at dei tilsette er i stand til å gjennomføre sine arbeidsoppgåver i samsvar med lover, krav og forventningar.

[64] *Internkontroll og informasjonssikkerhet.* Datatilsynet. Publisert 23.06.2018. https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/

Vedlegg 3: Sentrale dokument og litteratur

Lov og forskrift

- Justis- og beredskapsdepartementet: Lov om behandling av personopplysninger (personopplysningsloven). LOV-2018-06-15-38
- Kommunal- og moderniseringsdepartementet: Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften). FOR-2004-06-25-988

Rettleiarar og standardar

- Diverse rettleiingsmateriell frå Datatilsynet
- Diverse rettleiingsmateriell Direktorat for forvaltning og IKT (Difi)
- ISO/IEC 27001:2013

Dokumenter frå fylkeskommunen

- Styringssystem for informasjonstryggleik og personvern i Vestland fylkeskommune, inkludert følgjande godkjente dokument:
  - Informasjonssikkerheit og personvern i Vestland fylkeskommune
  - Organisering av informasjonstryggleik
  - Etterleving av informasjonssikkerheit i VLFK
  - Handbok for informasjonssikkerheit og personvern for Vestland fylkeskommune
  - IT-sikkerheitsreglar for tilsette og eksterne i Vestland fylkeskommune
  - Clean Desk Policy
  - Retningslinjer for leverandørstyring og IT-anskaffingar
  - Informasjonssikkerheit og personvern til innkjøp v. utlysing av anbod
  - Passord policy Vestland fylkeskommune
  - Tilgangskontroll i Vestland fylkeskommune
- Risikovurderingar, inkludert:
  - Risikovurderingar av behandlingar av personopplysningar
  - Personvernkonsekvensvurderingar
  - ROS av informasjonssystem
- Personvernerklæringar
- Protokollar over behandlingar av personopplysningar
- Prosedyrar, rutinar og retningslinjer knytt til personvern og informasjonstryggleik som ikkje inngår i styringssystemet, inkludert:
  - Avviksbehandling
  - Teiepliktserklæring
  - Fråsegn og teieplikt
  - *Retningslinjer for innhenting og tilbaketrekking av samtykke*,
  - *Retningslinjer for kva for og korleis informasjonen skal gjevast til den registrerte ved innhenting av personononopplysningar*,
  - *Retningslinjer og rutinar for sletting*
  - Mal for databehandlaravtalar
- Prosedyrar, rutinar og retningslinjer knytt til personvern og informasjonstryggleik i utkastsform, inkludert:
  - Prosedyre for risikovurdering og PIA (personvernkonsekvensvurdering)
  - VLFK tryggleiksarkitektur
  - Rutine for ny behandling av personopplysningar
  - Rutine ved førespurnad om innsyn i personopplysningar
  - Rutine ved førespurnad om dataportabilitet
  - Sjekkliste – databehandlaravtalar
  - Rutine for hensiktsmessig logging i informasjonssystem
  - Rutine for tilgangsstyring

Deloitte.