Deloitte.

# Forvaltningsrevisjon | Vestland fylkeskommune

Informasjonstryggleik

Prosjektplan/engagement letter

April 2020

«Forvaltningsrevisjon av informasjonstryggleik - prosjektplan»

April 2020

Prosjektplan utarbeidet for Vestland fylkeskommune av Deloitte AS.

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

# Innhald

# 1. Føremål og problemstillingar

## 1.1 Bakgrunn

Deloitte har i samsvar med bestilling frå kontrollutvalet 21. april i sak 35/20 utarbeidd ein prosjektplan for forvaltningsrevisjon av informasjonstryggleik i Vestland fylkeskommune.

## 1.2 Føremål og problemstillingar

Føremålet med prosjektet er 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 er òg eit føremål å undersøkje korleis fylkeskommunen praktiserer informasjonstryggleik med omsyn til konfidensialitet og tilgangsstyring, å undersøkje i kva grad fylkeskommunen etterlever sentrale krav i ny personvernlovgjeving, samt å undersøkje dei tilsette sin kompetanse på området.

Med bakgrunn i føremålet er det utarbeidd følgjande problemstillingar som vil bli 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. retningsliner og rutinar for informasjonstryggleik?
   c) I kva grad blir ev. retningsliner og rutinar for informasjonstryggleik følgt?

## 1.3 Avgrensingar

I undersøkingane av informasjonstryggleik vil revisjonen primært fokusere på krav stilt til handsaming og sikring av personopplysningar. Personopplysningslova og -forordninga (GDPR) stiller strenge krav til handsaming og sikring av slike opplysningar, og ein lekkasje av denne typen informasjon kan få store konsekvensar, både for fylkeskommunen og personane som blir råka. Ein gjennomgang av rutinar på dette området vil likevel også kunne omfatte rutinar knytt til andre sensitive eller fortrulege opplysningar.

Revisjonen vil ikkje gjennomføre undersøkingar, testingar eller analysar av teknisk konfigurasjon, tryggingstiltak eller operative driftsrutinar.

# 2. Revisjonskriterier

## 2.1 Innleiing

Revisjonskriteria vil bli henta frå og utleia av autoritative kjelder, rettsreglar, politiske vedtak og fastsette retningslinjer. Revisjonskriteria under er ikkje uttømmande for kva som kan vere relevant i forvaltningsrevisjonen. Andre kriterium vil kunne bli nytta dersom det er naudsynt for å få ei fullstendig undersøking og vurdering av problemstillingane.

## 2.2 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.

## 2.3 Krav i lov og forskrift

Regelverket knytt til informasjonstryggleik omfattar mellom anna personopplysningsloven.[1] Denne tredde i kraft 20. juli 2018, og gjennomfører EU si personvernforordning – kjend som GDPR[2] – 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.[3] 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).

---

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

### 2.3.1 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», 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.»

Personvernforordninga artikkel 32 nr. 1 stiller vidare krav om informasjonstryggleik ved behandling av personopplysningar. 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.

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.

### 2.3.2 Ytterlegare krav i personvernforordninga

Personvernforordninga stiller krav om 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.

Personvernforordninga pålegg fylkeskommunen å utpeike eit personvernombod, jf. artikkel 37 bokstav a. Artikkel 38 regulerer stillingstilhøva for personvernombodet, og det går mellom anna fram der at fylkeskommunen skal sikre at personvernombodet blir involvert i rett tid i alle spørsmål som gjeld personopplysningar (nr. 1), at fylkeskommunen skal stille tilstrekkeleg ressursar til rådigheit for at personvernombodet kan gjennomføre oppgåvene pålagt stillinga i personvernforordninga artikkel 38 (nr. 2), at personvernombodet skal vere uavhengig og rapportere direkte til fylkesrådmannen (nr. 3), og at personvernombodet er bunde av teieplikt (nr. 5).

Personvernombodet sine lovpålagte oppgåver går fram av artikkel 39. Her går det fram at personvernombodet mellom anna skal kontrollere at personvernforordninga blir overhaldt (bokstav b), gi råd om vurdering av personvernkonsekvensar (bokstav c), og samarbeide med Datatilsynet (bokstav d).

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), føremålet 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 behandlinga 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 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.

### 2.3.3 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*[4] 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. 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.

---

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

### 2.3.4 Anna regelverk

I tillegg til krava i personvernforordninga og eForvaltningsforskrifta er det også fleire andre reglar knytt til informasjonstryggleik som er relevant for fylkeskommunen. Krava i desse regelverka er i nokon grad overlappande med krava til eit styringssystem for informasjonstryggleik.

I helseregisterlova er det gitt konkrete føringar knytt til behandlinga av helseopplysningar, og her kjem det mellom anna fram konkrete krav knytt til informasjonstryggleik (§ 16). Det er utarbeidd ein norm for informasjonstryggleik i helse-, omsorgs- og sosialsektoren (Norma), som mellom anna omfattar tannhelse, og som stiller krav med utgangspunkt i både personopplysningsforskrifta og helseregisterlova.

## 2.4 Fylkeskommunale styringsdokument og vedtak

Relevante fylkeskommunale styringsdokument og vedtak kan bli nytta som revisjonskriterium.

# 3. Metode

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

## 3.1 Dokumentanalyse

Rettsreglar og kommunale vedtak vil bli 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.

## 3.2 Intervju

For å få supplerande informasjon til skriftlege kjelder vil Deloitte intervjue utvalde personar frå Vestland fylkeskommune som er involvert i eller har ansvar for informasjonstryggleik i ulike delar av organisasjonen. Vi tek sikte på å gjennomføre ca. 5-7 intervju.

## 3.3 Spørjeundersøking

Revisjonen vil gjennomføre ei elektronisk spørjeundersøking blant eit utval tilsette i Vestland fylkeskommune. Føremålet med spørjeundersøkinga er å kartleggje i kva grad dei tilsette har kjennskap til og følgjer etablerte rutinar knytt til informasjonstryggleik.

## 3.4 Nettfiskeforsøk

For å teste i kva grad dei tilsette i fylkeskommune har kjennskap til retningslinjer og rutinar for informasjonssikkerhet (problemstilling 5), vil revisjonen gjennomføre eit kontrollert nettfiskeforsøk.[5] Revisjonen sender då falske e-postar til dei tilsette i fylkeskommunen, for å undersøkje i kva grad dei følgjer retningslinjer knytt til trygg bruk av e-post.

## 3.5 Verifisering og høyring

Oppsummering av intervju vil bli sendt til dei intervjua for verifisering. Det er informasjon frå dei verifisert intervjureferata som vil bli nytta i rapporten. Faktadelen i rapporten vil bli sendt til fylkeskommunen for verifisering. Deretter vil heile rapporten, inkludert vurderingsdel og forslag til tiltak, bli sendt til fylkesrådmannen for uttale. Fylkesrådmannen sin høyringsuttale vil bli vedlagt den endelege rapporten som blir sendt til kontrollutvalet.

[5] Nettfisking blir òg kalla «phishing» eller «phisking».

# 4. Tid og ressursbruk

## 4.1 Nøkkelpersonell

Birte Bjørkelo er oppdragsansvarleg partnar på oppdraget. I tillegg vil teamet bestå av prosjektleiar Frode Løvlie, og prosjektmedarbeidarar Kjersti Gjuvsland og Samson Johnsen. Deloitte har sett saman eit team som sikrar at prosjektet blir gjennomført i samsvar med gjeldande retningsliner, samt med nødvendig kompetanse og erfaring innanfor kommunal revisjon.

## 4.2 Ressursbruk

Med utgangspunkt i prosjektet sin karakter og planen som er lagt for korleis prosjektet skal bli gjennomført vil det ta totalt 445 timar å gjennomføre prosjektet. Dette inkluderer førebuing av prosjektet, utarbeiding av problemstillingar og prosjektplan, førebuing og gjennomføring av datainnsamling, analyse av data og utarbeiding og kvalitetssikring av rapport. Timetalet omfattar også presentasjon av ferdig rapport for kontrollutvalet.

Timeestimatet inkluderer ikkje førebuing og gjennomføring av presentasjon i fylkestinget. Ein eventuell presentasjon av rapporten i fylkestinget vil bli fakturert etter medgått tid, inntil 6 timar i tillegg til det totale timetalet som er presentert over.

Sjå vedlegg for oversikt over timefordeling.

## 4.3 Gjennomføringsplan

Oppstart av prosjektet vil vere ultimo mai 2020, og rapporten vil vere klar for oversending til kontrollutvalet ved sekretariatet innan utgangen av november 2020. For å kunne gjennomføre prosjektet innan denne fristen og med stipulert timebruk er det nødvendig at fylkeskommunen sender over etterspurt dokumentasjon innan dei fristar som blir satt, og at utvalde personar stiller til og verifiserer intervju.

Fakturering av kostnadane ved prosjektet vil skje i samsvar med avtale mellom Vestland fylkeskommune og Deloitte.

Bergen, 29. april 2020

Birte Bjørkelo

Oppdragsansvarlig partnar

Deloitte.