Forvaltningsrevisjon
Januar 2026

Informasjonssikkerhet og personvern

Buskerud fylkeskommune

Viken
kommunerevisjon

Sammendrag

Forvaltningsrevisjon er utført av Viken kommunerevisjon IKS for Buskerud fylkeskommune, med tema Personvern og informasjonssikkerhet. Revisjonen ble vedtatt av kontrollutvalget 21. januar 2025, sak 3/25, på bakgrunn av høy risiko knyttet til informasjonssikkerhet og personvern, særlig i forhold til IKT-systemer forvaltet av FRID IKS.

Formålet med revisjonen er å vurdere om fylkeskommunen har en tilfredsstillende informasjonssikkerhet, og om fylkeskommunen har gjennomført de nødvendige steg som er pålagt for å kunne være i stand til å sikre et tilfredsstillende vern av fysiske personer i forbindelse med behandling av personopplysninger.

Metode og gjennomføring
Forvaltningsrevisjonen er gjennomført av egne ansatte i henhold til "RSK 001 Standard for forvaltningsrevisjon" og basert på dokumentanalyse og intervjuer med 20 ansatte og ledere i organisasjonen. Dokumentanalysen inkluderte styringssystemer, avtaler, DPIA og risikovurderinger, mens intervjuene dekket ulike roller som systemeiere, personvernombud, ledere og ansatte med ansvar/oppgaver innen informasjonssikkerhet og personvern.

Datamaterialet vurderes som gyldig og pålitelig, med triangulering mellom dokumentasjon og flere uavhengige intervjuer. Utkast til rapport er faktaverifisert av fylkeskommunen.

Revisjonskriterier og problemstillinger
Revisjonen bygger på kommuneloven, personopplysningsloven, GDPR, veiledere fra Datatilsynet og KINS, samt lokale vedtak og retningslinjer. To hovedproblemstillinger ble utledet:

- Har fylkeskommunen etablert tilfredsstillende informasjonssikkerhet, herunder internkontroll i henhold til kommuneloven?
- Har fylkeskommunen etablert tilfredsstillende vern av fysiske personer ved behandling av personopplysninger, inkludert databehandleravtaler, risikovurderinger, DPIA og involvering av personvernombudet?

Hovedfunn
Buskerud fylkeskommune har etablert et styringssystem for informasjonssikkerhet og personvern basert på ISO-standarder, med rutiner for avvikshåndtering, risikovurderinger og databehandleravtaler. Arbeidet er omfattende, men preges av mangler innen risikovurderinger, kompetanse og rolleavklaringer, særlig etter delingen av Viken. Det er igangsatt forbedringsprosesser, og en tiltaksplan skal lukke avvik innen utgangen av 2026.

Personvernombudet har en definert og uavhengig rolle, men involveres ofte for sent i prosesser. Databehandleravtaler og enkelte risikovurderinger er etablert, men flere systemer mangler oppdaterte vurderinger og oversikt. Fysisk lagring av sensitive opplysninger uten tilstrekkelig kontroll utgjør en risiko. Fylkeskommunen jobber med å styrke rutiner, kompetanse og ansvar, men det kreves fortsatt systematisk innsats for å oppfylle lovkravene fullt ut.

Anbefalinger

Med bakgrunn i vår gjennomgang vil vi anbefale Buskerud fylkeskommune følgende:

- sikre at det etableres en tilstrekkelig internkontroll for arbeidet med informasjonssikkerhet og personvern.
- sikre implementering av internkontrollen for arbeidet med informasjonssikkerhet og personvern.
- sørge for at det utarbeides databehandleravtaler der det er påkrevd.
- sørge for at det utarbeides ROS-analyser og personvernkonsekvensvurderinger der det foreligger lovkrav om det.
- sørge for at personvernombudet blir involvert til rett tid i alle spørsmål som gjelder pålagte og relevante prosesser knyttet til personopplysninger.

Høringsprosess

Et utkast til rapport har blitt oversendt Fylkeskommunedirektøren til uttalelse. Fylkeskommunedirektørens uttalelse datert 9. januar 2026 er vedlagt rapporten.

Innhold

1. Innledning

1.1. Bakgrunn for prosjektet

Kontrollutvalget i Buskerud fylkeskommune vedtok 21. januar 2025 (sak 3/25) at Viken kommunerevisjon IKS (VKR) skulle gjennomføre en forvaltningsrevisjon om informasjonssikkerhet og personvern.

Prosjektet har sin bakgrunn i områder prioritert av kontrollutvalget under sin behandling av ROV (risiko- og vesentlighetsvurdering). I behandlingen av saken prioriterte kontrollutvalget dette området, og bestilte et forslag til prosjektplan for denne forvaltningsrevisjonen.

I ROV fremkommer følgende om revisors vurdering av risiko for tema «Informasjonssikkerhet og personvern»:

«Revisjonen har konkludert med at risikoen er høy på området informasjonssikkerhet og personvern. Det er både risiko knyttet til å etablere systemer og rutiner internt i Buskerud fylkeskommune, men også knyttet til om området ivaretas i forbindelse med IKT-systemer forvaltet av FRID IKS. En eventuell forvaltningsrevisjon bør derfor inkludere FRID IKS og gjennomføres i samråd med kontrollutvalgene i de øvrige eierfylkeskommunene (Akershus og Østfold)»

Risiko er vurdert som høy.

1.2. Formål og problemstillinger

Revisjonens formål er å vurdere om fylkeskommunen har en tilfredsstillende informasjonssikkerhet, og om fylkeskommunen har gjennomført de nødvendige steg som er pålagt for å kunne være i stand til å sikre et tilfredsstillende vern av fysiske personer i forbindelse med behandling av personopplysninger.

Revisjonen har følgende problemstillinger:

- Har fylkeskommunen sikret at det er etablert en tilfredsstillende informasjonssikkerhet?
- Har fylkeskommunen sikret at det er etablert et tilfredsstillende vern av fysiske personer i forbindelse med behandling av personopplysninger?

1.3. Avgrensning av undersøkelsen

Som det går fram av problemstillingene i kulepunktene i kapittel 1.2, er det vedtatt relativt konkrete problemstillinger for forvaltningsrevisjonen. Vi presiserer at prosjektet kun tar for seg de områder og temaer som faller inn under de problemstillingene som fremgår av kapittel 1.2. Vurderinger og konklusjoner omfatter derfor bare disse avgrensede definerte områdene eller temaene.

1.4. Leseveiledning

Innledningsvis vil revisjonen vise til at når Viken ble delt, ble all strategisk og operativ kompetanse på digitaliseringsområdet lagt til FRID IKS og ikke fylkeskommunen. Buskerud fylkeskommune har derfor måtte

bygge opp både egen kompetanse og egen metodikk. Fylkeskommunen har iverksatt dette arbeidet og det har pågått gjennom prosjektperioden for denne forvaltningsrevisjonen.

2. Metode

Forvaltningsrevisjon utført av Viken kommunerevisjon IKS gjennomføres, dokumenteres, kvalitetssikres og rapporteres i samsvar med kommuneloven og god kommunal revisjonsskikk.[1]

Prosjektet er gjennomført av revisjonens egne ansatte på bakgrunn av kravene som stilles til gjennomføring av forvaltningsrevisjon som prosjekt. Det vil si at gjennomgangen er basert på "RSK 001 Standard for forvaltningsrevisjon" som er vedtatt av Norges Kommunerevisorforbund (NKRF).

Samtlige revisorer som har deltatt i prosjektet er løpende vurdert å være uavhengige, habile og objektive, jf. RSK 001 punkt 3.

Informasjonen som er presentert i dette prosjektet, er hentet inn gjennom dokumentanalyse og intervjuer.

Vi viser kapittel 1.3 for eventuelle avgrensinger i prosjektets omfang.

2.1. Dokumentanalyse

Dokumentene som er analysert er knyttet til fylkeskommunens arbeid med informasjonssikkerhet og personvern. Fylkeskommunen har sendt inn relevant dokumentasjon som oversikt over kurs, avtale med FRID, overordnet styringssystemer, informasjon fra Personvernombudet, dokumentasjon av styringssystemer, DPIA og Ros-analyser med mere.

Fylkeskommunen har delt område hvor aktuell dokumentasjon i forhold til prosjektet er lagret med revisjonen.

2.2. Intervju

I undersøkelsen er det gjennomført intervju med totalt 20 ansatte og ledere i organisasjonen med oppgaver knyttet til informasjonssikkerhet og personvern

Vi har snakket med følgende:

Rolle	Antall personer
Systemeier Visma in school	1
Leder dokumentsenteret	1
Systemansvarlig Vigo-OT	1
Ansatte som arbeider med barn med nedsatt funksjonsevne på VGS	2
Personvernombudet	1

[1] God kommunal revisjonsskikk i forvaltningsrevisjon og eierskapskontroll kommer til uttrykk først og fremst i RSK 001 Standard for forvaltningsrevisjon og RSK 002 Standard for eierskapskontroll. Gjeldende standarder er fastsatt av Norges Kommunerevisorforbunds styre høsten 2020. Standarden bygger på norsk regelverk og internasjonale prinsipper og standarder, fastsett av International Organization of Supreme Audit Institutions (INTOSAI) og Institute of Internal Auditors (IIA).

Økonomisjef	1
Ansatte – TT-systemet	3
Direktør Frid og personvernrådgiver	2
Direktør for kommunikasjon, sikkerhet og myndighetskontakt	1
Fagansvarlig informasjonssikkerhet og personvern	1
Porteføljestyrer	1
Rektorer	2
Systemansvarlige Opus	2
Klinikkleder for tannhelse og fylkestannlege	1

Det er utarbeidet en intervjuguide med temaer hvor alle problemstillingene berøres. Hvert tema er utdypet med momenter for å sikre at vi berører de aspekter som er relevant for revisjonen. På denne måten struktureres intervjuet slik at man snakker om et tema, men innenfor dette er det en frihet til å velge den rekkefølgen som faller intervjuobjektet mest naturlig.

Revisjonen har skrevet referat fra hvert intervju. Intervjureferatene er verifisert av de som er intervjuet.

2.3. Dataenes pålitelighet og gyldighet

Gyldighet og pålitelighet
Revisjonen mener at datamaterialet samlet sett gir et godt grunnlag for våre beskrivelser av de aktuelle områder.

Vi mener at datamaterialet vi har samlet inn har tilstrekkelig gyldighet (validitet) og pålitelighet (relabilitet) til å besvare de vedtatte problemstillingene.

Gyldighet (validitet) ut fra at vi mener det er samsvar mellom problemstillingene og revisjonskriteriene for undersøkelsen, og de data som er samlet inn. Det vil si at revisjonen har stilt de riktige spørsmålene for å få svar på det vi ønsker å undersøke.

For å sikre dataenes pålitelighet (relabilitet) har vi søkt å hente informasjon fra relevante ansatte i fylkeskommunen, samt politikerne.

Revisjonen har gjennomgått autoritative og relevante dokumenter fra fylkeskommunen som er verifiserbare og kvalitetssikret av de aktuelle instansene.

I denne forvaltningsrevisjonen er det benyttet et stort antall intervjuer som kilde til informasjon. Når flere uavhengige intervjuobjekter gir sammenfallende opplysninger, styrkes både validiteten og reliabiliteten i datagrunnlaget. Sammenfallende informasjon indikerer at opplysningene ikke er enkeltstående, men reflekterer en felles oppfatning eller praksis.

Gyldigheten vurderes som høy når opplysningene er relevante for revisjonens problemstillinger og kan knyttes direkte til dokumentert praksis. Dokumentasjonen som er innhentet, fungerer som en kontrollmekanisme og bidrar til triangulering, noe som ytterligere øker troverdigheten. Likevel må det tas høyde for at intervjudata kan være påvirket av subjektive oppfatninger. Derfor er kombinasjonen av intervjuer og skriftlig dokumentasjon avgjørende for å sikre et robust og etterprøvbart grunnlag.

Forvaltningsrevisjonen viser høy grad av sammenfall mellom informasjonen som er gitt fra respondentene og dokumentgjennomgangen. Denne trianguleringen mener revisjonen bidrar til å styrke dataenes pålitelighet. Samtidig er det et argument for at dataene har høy grad av gyldighet.

Verifisering
Revisjonen sendte rapporten på fakta verifisering til lederne som har deltatt i revisjonen. Det ble gjennomført møte med fylkeskommunen den 5. desember 2025, der fakta i rapporten ble gjennomgått. Revisjonen mottok tilbakemelding på fakta fra fylkeskommunen den 15.12.2025.

Revisjonen har som følge av faktagjennomgang tatt inn alle tilbakemeldinger i rapporten. Endringene har ikke hatt noen betydning for vurdering og konklusjonen på problemstillingene.

Høringsprosess
Et utkast til rapport har blitt oversendt Fylkeskommunedirektøren til uttalelse. Fylkeskommunedirektørens uttalelse datert 9. januar 2026 er vedlagt rapporten.

3. Revisjonskriterier

Kilder for revisjonskriteriene [2] :

Lov og forskrift:

- LOV 2018-06-22 nr 83 – Lov om kommuner og fylkeskommuner (kommuneloven)
- LOV 2018-12-20 nr 116, Lov om behandling av personopplysninger (personopplysningsloven)
- EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning)

Sentrale føringer:

- Prop. 56 LS (2017–2018), Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen
- Veiledere fra Datatilsynet
- Veiledere fra KINS – Foreningen kommunal informasjonssikkerhet

Lokale føringer:

- Fylkeskommunale vedtak, rutiner og retningslinjer

På bakgrunn av problemstillingene og relevante krav i kildene, har vi utledet følgende revisjonskriterier for vår gjennomgang av fylkeskommunens arbeid med Personvern og Informasjonssikkerhet. Kriteriene er ikke nødvendigvis uttømmende for ethvert krav som stilles til alle sider av arbeidet. Kriteriene er oppstilt etter revisjonens vurdering av hva som er det sentrale, basert på en vurdering av virksomhetens egenart og regelverket den forvalter.

Problemstilling 1

Har fylkeskommunen sikret at det er etablert en tilfredsstillende informasjonssikkerhet?

Kilder og begrunnelse:
Fylkeskommunen skal ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges. Kommunedirektøren i fylkeskommunen er ansvarlig for internkontrollen jf. kommuneloven §25-1.

Alle deler av administrasjonen er omfattet av kravet om internkontroll. Kravet om internkontroll gjelder for alle lovpålagte plikter fylkeskommunen har.

Internkontrollen skal være systematisk og tilpasses virksomhetens størrelse, egenart, aktiviteter og risikoforhold.

Ved internkontroll etter kommuneloven § 25-1 skal fylkeskommunedirektøren:

[2] Revisjonskriterier er en samlebetegnelse for krav og forventninger som benyttes for å vurdere kommunens virksomhet, økonomi, produktivitet, måloppnåelse, regeletterlevelse osv. Sammenholdt med faktabeskrivelsen danner revisjonskriteriene basis for de analyser og vurderinger som foretas, de konklusjoner som trekkes, og de er et viktig grunnlag for å kunne dokumentere avvik eller svakheter.

a) utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering
b) ha nødvendige rutiner og prosedyrer
c) avdekke og følge opp avvik og risiko for avvik
d) dokumentere internkontrollen i den formen og det omfanget som er nødvendig
e) evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.

Her har vi utledet følgende revisjonskriterium:

- **Fylkeskommunen skal ha etablert internkontroll for arbeidet med informasjonssikkerhet.**

Problemstilling 2

Har fylkeskommunen sikret at det er etablert et tilfredsstillende vern av fysiske personer i forbindelse med behandling av personopplysninger?

Kilder og begrunnelse:
Det følger av personopplysningsloven § 4 at loven og personvernforordningen gjelder for behandling av personopplysninger som utføres i forbindelse med aktivitetene ved virksomheten til en behandlingsansvarlig eller en databehandler.

I Artikkel 28 i GDPR fremkommer det at dersom en behandling skal utføres på vegne av en behandlingsansvarlig, skal den behandlingsansvarlige bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning og vern av den registrertes rettigheter.

Databehandleravtaler er påkrevd når en virksomhet (som fylkeskommunen) setter ut behandling av personopplysninger til en ekstern part (databehandler). Dette følger av artikkel 28 i GDPR og personopplysningsloven § 18.

Avtalen må være oppdatert og konkret, spesielt når behandlingen er omfattende, sensitiv eller risikofylt. Det er ikke nok med generelle formuleringer – avtalen må spesifisere formål, type data, sikkerhetstiltak, og eventuelle underdatabehandlere

Fylkeskommunen som behandlingsansvarlig har ansvar for at databehandleren følger regelverket. Dette inkluderer å sikre at avtalen er oppdatert ved endringer i behandling, systemer, leverandører eller lovgivning.

Databehandleren har også plikter, blant annet til å gjennomføre risikovurderinger og følge sikkerhetskrav. Disse må være dokumentert i avtalen.

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 personopplysningsvernet. En vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer, jf artikkel 35 nr. 1.

Artikkel 35 nr. 1 angir vurderingskriteriet for når den behandlingsansvarlige plikter å gjennomføre en DPIA, nemlig dersom behandlingen sannsynligvis vil medføre en høy risiko for fysiske personers rettigheter og friheter. Hvorvidt det foreligger en slik sannsynlighet for høy risiko, beror på en konkret, skjønnsmessig vurdering. Artikkel 35 nr. 3 angir situasjoner som alltid krever en DPIA.

Den behandlingsansvarlige skal rådføre seg med personvernombudet, dersom et personvernombud er utpekt, i forbindelse med utførelsen av en vurdering av personvernkonsekvenser.

I nr. 3 i artikkel 35 står det at en vurdering av personvernkonsekvenser som nevnt i nr. 1 skal særlig være nødvendig i følgende tilfeller:

a) en systematisk og omfattende vurdering av personlige aspekter ved fysiske personer som er basert på automatisert behandling, herunder profilering, og som danner grunnlag for avgjørelser som har rettsvirkning for den fysiske personen eller på lignende måte i betydelig grad påvirker den fysiske personen,
b) behandling i stor skala av særlige kategorier av opplysninger som nevnt i artikkel 9 nr. 1, eller av personopplysninger om straffedommer og lovovertredelser som nevnt i artikkel 10, eller
c) en systematisk overvåking i stor skala av et offentlig tilgjengelig område.

Det følger av nr. 7 at vurderingen skal minst inneholde

a) en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen, herunder, dersom det er relevant, den berettigede interessen som forfølges av den behandlingsansvarlige,
b) en vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene,
c) en vurdering av risikoene for de registrertes rettigheter og friheter som nevnt i nr. 1, og
d) de planlagte tiltakene for å håndtere risikoene, herunder garantier, sikkerhetstiltak og mekanismer for å sikre vern av personopplysninger og for å påvise at denne forordning overholdes, idet det tas hensyn til de registrertes og andre berørte personers rettigheter og berettigede interesser.

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

a) noens personlige forhold
b) tekniske innretninger, produksjonsmetoder, forretningsmessige analyser og beregninger og forretningshemmeligheter ellers når opplysningene er av en slik art at andre kan utnytte dem i sin egen næringsvirksomhet
c) sikkerhetstiltak etter personvernforordningen artikkel 32
d) enkeltpersoners varsling om overtredelser av loven her.

Den behandlingsansvarlige og databehandleren skal sikre at personvernombudet på riktig måte og i rett tid involveres i alle spørsmål som gjelder vern av personopplysninger, jf. artikkel 38.

Den behandlingsansvarlige og databehandleren skal utpeke et personvernombud når

a) behandlingen utføres av en offentlig myndighet, jf. artikkel 37.

Personvernombudet skal minst ha følgende oppgaver:

a) informere og gi råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har i henhold til denne forordning, og i henhold til andre av Unionens eller medlemsstatenes bestemmelser om vern av personopplysninger,
b) kontrollere overholdelsen av denne forordning, av andre av Unionens eller medlemsstatenes personvernregler og den behandlingsansvarliges eller databehandlerens personvernretningslinjer, herunder fordeling av ansvar, holdningsskapende tiltak og opplæring av personellet som er involvert i behandlingsaktivitetene, og tilhørende revisjoner,

c) på anmodning gi råd om vurderingen av personvernkonsekvenser og kontrollere gjennomføringen av den i henhold til artikkel 35,
d) samarbeide med tilsynsmyndigheten,
e) fungere som kontaktpunkt for tilsynsmyndigheten ved spørsmål om behandlingen, herunder forhåndsdrøftingene nevnt i artikkel 36, og ved behov rådføre seg med tilsynsmyndigheten om eventuelle andre spørsmål.

Personvernombudet skal ved utførelsen av sine oppgaver ta behørig hensyn til risikoene forbundet med behandlingsaktivitetene, idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i jf. artikkel 39.

Fylkeskommuner skal ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges. Kommunedirektøren i fylkeskommunen er ansvarlig for internkontrollen jf. kommuneloven §25-1.

Alle deler av administrasjonen er omfattet av kravet om internkontroll. Kravet om internkontroll gjelder for alle lovpålagte plikter fylkeskommunen har.

Internkontrollen skal være systematisk og tilpasses virksomhetens størrelse, egenart, aktiviteter og risikoforhold.

Her har vi utledet følgende revisjonskriterier:

- **Databehandleravtaler skal inngås når fylkeskommunen setter ut behandling av personopplysninger til en ekstern part (databehandler).**
- **Fylkeskommunen som behandlingsansvarlig skal påse at databehandler følger regelverket, herunder blant annet gjennomfører risikovurderinger og personkonsekvensvurdering der det behandles personopplysninger.**
- **Fylkeskommunen skal sikre at personvernombudet på riktig måte og i rett tid involveres i alle spørsmål som gjelder vern av personopplysninger.**
- **Fylkeskommunen skal ha etablert internkontroll for arbeidet med personopplysninger og Personvernombudets rolle.**

4. Internkontroll - informasjonssikkerhet og personvern

Dette kapittelet setter søkelys på problemstilling 1 og 2:

Har fylkeskommunen sikret at det er etablert en tilfredsstillende informasjonssikkerhet?

Har fylkeskommunen sikret at det er etablert et tilfredsstillende vern av fysiske personer i forbindelse med behandling av personopplysninger?

Til problemstilling 1 har vi i kapittel 3 utledet følgende revisjonskriterium:

- Fylkeskommunen skal ha etablert internkontroll for arbeidet med informasjonssikkerhet.

Til problemstilling 2 har vi i kapittel 3 utledet følgende revisjonskriterium:

- Fylkeskommunen skal ha etablert internkontroll for arbeidet med personopplysninger og Personvernombudets rolle.

4.1. Fakta

Buskerud fylkeskommune opplyser å ha etablert et helhetlig rammeverk for internkontroll knyttet til informasjonssikkerhet og personvern. Rammeverket omfatter organisatoriske, tekniske og administrative tiltak som skal sikre etterlevelse av gjeldende regelverk, herunder personopplysningsloven og personvernforordningen (GDPR).

Buskerud fylkeskommune opplyser å ha etablert et styringssystem for informasjonssikkerhet og personvern (ISMS) som skal ivareta internkontroll på systemnivå. Systemet opplyses å være strukturert i henhold til internasjonale standarder og nasjonale krav, og omfatter styrende, gjennomførende og kontrollerende dokumenter.

Styringssystemets struktur og formål
Styringssystemet er basert på ISO/IEC 27001 og ISO/IEC 27701, og skal sikre konfidensialitet, integritet og tilgjengelighet i all informasjonsbehandling

Systemet omfatter:

- ***Styrende dokumenter**: fastsetter retning og mål.*
- ***Gjennomførende dokumenter**: beskriver implementering og drift.*
- ***Kontrollerende dokumenter**: evaluerer og overvåker effektivitet*

Ledelsesforankring og ansvar
Styringssystemet er vedtatt av strategisk ledergruppe. Fylkeskommunedirektøren har overordnet ansvar for innhold og etterlevelse. Øvrige roller og ansvar er definert i eget styringsdokument.

Risikostyring og sikkerhetsrevisjoner
Fylkeskommunen gjennomfører risikovurderinger og sikkerhetsrevisjoner i henhold til godkjente rutiner. Alle informasjonssystemer kritikalitetvurderes, og krav til tilgjengelighet inngår i vurderingen.

Etterlevelse og forbedring
Styringssystemet skal sikre samsvar med gjeldende lovverk, herunder personopplysningsloven og GDPR. Det legges til rette for kontinuerlig forbedring gjennom regelmessig evaluering av prosesser og tiltak.

Personvern og behandlingsgrunnlag
Fylkeskommunen skal behandle personopplysninger lovlig, rettferdig og åpent. Det skal foreligge rettslig grunnlag og formål før behandling igangsettes. Behandlingsprotokoller skal utarbeides per virksomhetsområde.

Dokumentkontroll og unntakshåndtering
Alle dokumenter i styringssystemet er underlagt versjonskontroll og beskyttes mot uautoriserte endringer. Unntak fra styringsdokumentet skal dokumenteres og godkjennes av fylkeskommunedirektøren.

Fylkeskommunen har også utarbeidet en rekke rutiner på personvern og informasjonssikkerhet, herunder:

- Rutine for avvik innen informasjonssikkerhet og personvern
- Rutine for behandlingsprotokoll
- Rutine for ivaretakelse av personvern og informasjonssikkerhet v/anskaffelser
- Rutine for meldeplikt og informasjonsplikt
- Rutine for risikovurdering av behandlingen
- Rutine for vurdering av personvernkonsekvenser (DPIA)
- Rutine for filming, strømming og lydopptak.
- Rutine for oppstart av behandling av personopplysninger
- Sjekkliste for databehandler avtale (GDPR)
- Rutine for inngåelse av databehandleravtale

Disse rutinene angir blant annet formål, ansvar, fremgangsmåte og tiltak/aktivitet. Det fremkommer også når rutinen ble godkjent og det viser at de fleste av rutinene er etablert i 2025.

Buskerud fylkeskommune arbeider også med å etablere en rekke rutiner. Arbeidet vil bli ferdigstilt i løpet av 2026.

- Sikkerhetsinstruks for informasjonssikkerhet
- Styringsdokument for fjernarbeid
- Styringsdokument for fysisk sikkerhet
- Styringsdokument for IKT-beredskap for virksomhetskontinuitet
- Styringsdokument for personellsikkerhet
- Styringsdokument for styring av informasjonsverdi
- Styringsdokument for tilgangsstyring

Buskerud fylkeskommune har etablert, «*Styringsdokument for å ivareta de registrertes rettigheter»,* som definerer rammer og føringer for ivaretakelse av de registrertes rettigheter ved behandling av personopplysninger. Dokumentet gjelder for alle virksomheter og enheter i fylkeskommunen, inkludert fylkesadministrasjonen. Dokumentet angir:

> ***Ansvarsfordeling***
> *Fylkeskommunedirektøren har det overordnede ansvaret for behandling av personopplysninger, i tråd med delegasjonsreglement og styringsdokument for roller og ansvar.*
>
> *Avdelingsdirektører skal gjøre dokumentet kjent og implementere det i eget virksomhetsområde.*
>
> *Ledere med personalansvar skal sikre at ansatte kjenner til relevante dokumenter og rutiner.*
>
> ***Tiltak for internkontroll***
> *Fylkeskommunen har iverksatt følgende tiltak for å sikre internkontroll på området:*
>
> ***Informasjon til registrerte***
> *Informasjon om behandling av personopplysninger skal være tydelig, tilgjengelig og forståelig. Informasjon skal gis før eller samtidig med innsamling, tilpasset innsamlingsmetoden.*
>
> *Personvernerklæringer skal være kortfattede, åpne og tilpasset målgruppen.*
>
> ***Innsyn og utlevering***
> *Det er etablert sikre og effektive løsninger for innsynsforespørsler og utlevering, eksempelvis digitale skjemaer med sikker autentisering.*
>
> *Personopplysninger utleveres til digital postkasse for å sikre konfidensialitet og integritet.*
>
> ***Øvrige rettigheter***
> *Det er etablert mekanismer for samtykkehåndtering der dette er aktuelt.*
>
> *Rettigheter som korrigering, protest, begrensning og sletting håndteres gjennom sikre løsninger med dokumentasjon.*

Fylkeskommunen har også styringsdokumenter på områdene:

- Styringsdokument for behandling av personopplysninger
- Styringsdokument for klassifisering av informasjon
- Styringsdokument for roller og ansvar innen arbeidet med informasjonssikkerhet og personvern
- Styringsdokument for vurdering av systemkritikalitet
- Styringsdokumenter for kontinuerlig forbedring
- Styringsdokument for ivaretakelse av informasjonssikkerhet og personvern i leverandørforhold
- M.M

«*Styringsdokument for roller og ansvar innen arbeidet med informasjonssikkerhet og personvern*» inneholder informasjon om blant annet omfang, behandlingsansvar, FRID IKS, Sikkerhet- og beredskapsteam og hva de enkelte rollene knyttet til informasjonssikkerhet og personvern har av ansvar og oppgaver. Det gjelder helt fra leder nivå helt ut til de enkelte seksjoner/virksomheter og ansatte. Det fremgår at det er Direktør for kommunikasjon, sikkerhet og myndighetskontakt som har det overordnede ansvaret for å ivareta informasjonssikkerhet og personvern i fylkeskommunen og at det innebærer å utarbeide en oversikt over behandlingen av personopplysninger, en systemoversikt og at internkontrollsystemet er etablert og implementert. De fleste av styringsdokumentene er godkjent i 2025.

I innsendt dokumentasjon finner revisjonen også en veileder for utarbeidelse av personkonsekvensvurdering, retningslinjer for risikovurderinger og rutine for avvikshåndtering i fylkeskommunen. Det er også lagt ved Mal for risikovurderinger, personkonsekvensvurderinger og for vurdering av berettiget interesse.

Fylkeskommunen har inngått en avtale med FRID IKS[3] som omhandler IKT-utstyr (pc og pc-utstyr, samt AV/møteromsutstyr), infrastruktur, lisenser, fag- og fellessystemer, databehandleravtaler og annet som kreves for å levere IKT- og digitaliseringstjenester. Avtalen angir at det er Fylkeskommunen som er behandlingsansvarlig etter personopplysningsloven, mens FRID IKS er databehandler.

Fylkeskommunen tilbyr de ansatte e-læringskurs om cybersikkerhet. I 2024 var det 34% av de ansatte som gjennomførte kurset enten fult eller delvis. Fylkeskommunen har også planer om å gjennomføre samme kurs også i 2025.

Intervjuer

I intervjuer med ansatte og ledere kom det frem at fylkeskommunens arbeid med internkontroll innen informasjonssikkerhet og personvern fremstår som omfattende, men samtidig preget av flere utfordringer som krever oppfølging. Det blir sagt at organisasjonen har etablert enkelte rutiner, blant annet for involvering av personvernombudet ved nyanskaffelser, men at disse er ikke konsekvent implementert ved oppgraderinger og utviklingsprosjekter. Det arbeides derfor med å etablere faste rutiner som sikrer tidlig involvering i alle prosesser. Videre er det innført rutiner for håndtering av personvernrelaterte avvik, og rapporteringen har økt etter at nye prosedyrer ble tatt i bruk i 2024. Tannhelsetjenesten forteller at de har etablert egne rutiner for behandlingsprotokoller og ROS-analyser, ledet av personvernombudet.

Det fremkommer likevel i intervjuene at det samtidig avdekkes flere avvik og utfordringer. Det mangler risikovurderinger og Personkonsekvensvurdering (DPIA)for en rekke systemer, men dette arbeider fylkeskommunen med å etablere på revisjonstidspunktet. Kompetansenivået på personvern og informasjonssikkerhet blant systemeiere og ledere beskrives som noe manglende, og rollene mellom interne aktører og FRID er uklare. Manglende oversikt over systemkritikalitet og fravær av rutiner for loggkontroller og stikkprøver forsterker risikoen. Kostnadskutt hos FRID trekkes frem som en faktor som svekker sikkerhetsnivået og tjenesteleveransen.

Det blir også trukket frem i intervjuene at ansvarsområdene er delvis definert, men ikke alltid tydelige. Personvernombudet har en rådgivende rolle, men blir ofte involvert for sent og har ikke mandat til systematisk oppfølging av tiltak. FRID fungerer både som databehandler, rådgiver og kontraktsforvalter, men fullmaktene er uklare. Porteføljestyrerrollen er etablert for å styrke kontrollen over systemporteføljen og koordinere tiltak.

Gjennom intervjuene blir det påpekt at uklare ansvarsforhold og manglende styringsdokumenter, samt rutiner for fagområdet ikke er en ny problemstilling, da lite av dette ble overført fra Viken til nye Buskerud fylkeskommune. Det samme gjelder ROS-analyser og DPIA-vurderinger. Ved avviklingen av Viken ble all strategisk og operativ digitaliseringskompetanse plassert i FRID IKS, samtidig som ansvaret for å følge regelverket lå hos fylkeskommunen. Fylkeskommunen har derfor helt på nytt måttet bygge opp kompetanse, kapasitet og metodikk på området, i tillegg til å håndtere det operative mot FRID IKS. Dette arbeidet er fylkeskommunen ikke i mål med, men det er igangsatt en rekke forbedringsprosesser med god progresjon.

[3] FRID IKS

FRID IKS legger til at FRID vil utarbeide en ny tjenesteavtale for sine kunder i 2026. Personvern og sikkerhet vil beskrives som eget vedlegg til avtalen for å tydeliggjøre ansvar og rolle forbundet med områdene. I tillegg skal FRID IKS etablere sikkerhetsforum og personvernforum som følger opp ansvarsfordeling og påser at avtalen utvikles i tråd med behov. I forumene blir kundene inkludert.

Intervju med Direktør for kommunikasjon, sikkerhet og myndighetskontakt og Fagansvarlig Informasjonssikkerhet og personvern

Fylkeskommunen har gjennomført en gap-analyse mot ISO 27001:2022, ISO 27701 og NSMs grunnprinsipper for IKT-sikkerhet. Analysen har identifisert områder som skal prioriteres og videreutvikles i 2026. Arbeidet med å lukke avvik og forbedringspunkter pågår fortløpende, med dokumenterte tiltak, ansvarlige personer og tidsplaner. Målet er at alle tiltak skal være gjennomført innen utgangen av 2025, og resultatene vil danne grunnlag for interne revisjoner i andre kvartal 2026. Arbeidet er tett knyttet til kravene i personvernforordningen (GDPR) og nasjonale sikkerhetsprinsipper, og Datatilsynet involveres ved alvorlige avvik.

De forteller at det er flere forhold som belyser fylkeskommunens internkontroll innen informasjonssikkerhet og personvern. Arbeidet med risikovurderinger og personvernkonsekvensvurderinger (DPIA) er igangsatt, men ikke fullført, og det er tydelig at oversikten over tidligere analyser fra Viken mangler. Fagansvarlig Informasjonssikkerhet og personvern har fått ansvaret for å sikre at det etableres tekniske risikovurderinger og DPIA-er, samt kartlegge systemeiere og innkjøpsprosesser. Det er også utarbeidet et forslag til oversikt over risikovurderinger og DPIA-er i SharePoint, men dokumentasjonen er foreløpig begrenset og kvalitetssystemet brukes ulikt i organisasjonen, noe som gjør det vanskelig å få helhetlig oversikt.

De peker likevel på flere utfordringer. Det er behov for tydeliggjøring av roller som tjenesteeier og behovseier da forståelsen av disse varierer i organisasjonen. Tjenesteeier skal definere krav til informasjonssikkerhet og tilgangsstyring, men oppfølgingen er ujevn. Det mangler rutiner for loggkontroller og stikkprøver, og selv om styringsdokumenter finnes, er intern revisjon og bevisstgjøring nødvendig.

Ansvarsområdene er fordelt slik at Fagansvarlig Informasjonssikkerhet og personvern har en sentral rolle i risikovurderinger og DPIA-er, mens tjenesteeiere har ansvar for krav til informasjonssikkerhet, tilgangsstyring og oppfølging av loggkontroller. Porteføljeforvalter har en oversikt over systemeierskap, strategisk ledergruppe skal motta modenhetsvurdering og gap-analyse. Det er også varslet at krav til informasjonssikkerhet og personvern skal innarbeides i ny tjenestekatalog.

Når det gjelder risikovurderinger og sikkerhetsnivåer, er det gjennomført en gap-analyse mot ISO 27001:2022, ISO 27701 og NSMs grunnprinsipper for IKT-sikkerhet. Denne analysen har identifisert områder som skal prioriteres og videreutvikles i 2026, og arbeidet med å lukke avvik og forbedringspunkter pågår fortløpende. Alle funn er dokumentert med tiltak, ansvarlige og tidsplaner, med mål om ferdigstillelse innen utgangen av 2025. Resultatene fra analysen skal danne grunnlag for interne revisjoner i andre kvartal 2026. Buskerud fylkeskommunen har vurdert seg å ligge på digitaliseringstrinn 2,5 og det planlegges en modenhetsvurdering og gap-analyse for å definere kritiske systemer og ansvar.

Planlagte forbedringer inkluderer fullføring av ROS-analyser og DPIA-er, tydeliggjøring av roller og ansvar, kompetanseheving, bedre samling og tilgjengeliggjøring av dokumentasjon, utarbeidelse av en felles digitaliseringsstrategi for Buskerud, Akershus og Østfold, gjennomføring av interne revisjoner i 2026 og vurdering av anskaffelse av en egen løsning for styringssystem for informasjonssikkerhet.

Det skal utarbeides en tiltaksplan basert på risikovurderinger fra ledergruppen, og det legges opp til tydeligere rolleavklaringer og opplæringsprogram for å heve kompetansen. Anskaffelse av en løsning for

styringssystem vurderes, og en digitaliseringsstrategi skal bidra til å styrke internkontrollen og modenheten i organisasjonen.

4.2. Revisjonens vurdering og konklusjon

Revisjonskriteriene innebærer at fylkeskommunen skal ha etablert internkontroll for arbeidet med informasjonssikkerhet og personvern. Internkontrollen skal være systematisk og omfatte styrende, gjennomførende og kontrollerende tiltak som sikrer etterlevelse av gjeldende regelverk. Herunder personopplysningsloven og personvernforordningen (GDPR).

Buskerud fylkeskommune har etablert et helhetlig rammeverk for internkontroll på området. Rammeverket er strukturert i tråd med internasjonale standarder (ISO/IEC 27001 og ISO/IEC 27701) og nasjonale krav, og omfatter styringsdokumenter, operative rutiner og veiledninger. Det foreligger tydelige føringer for tilgangsstyring, logging, kryptering, lagring, avvikshåndtering og opplæring. Videre er det etablert et styringssystem (ISMS) som skal sikre konfidensialitet, integritet og tilgjengelighet i informasjonsbehandlingen. Ledelsesforankringen fremstår som tydelig, med fylkeskommunedirektøren som overordnet ansvarlig og definerte roller og ansvar i styringsdokumentene.

Det er også utarbeidet en rekke rutiner som dekker sentrale krav i personvernforordningen, herunder rutiner for behandlingsprotokoller, risikovurderinger, DPIA og avvikshåndtering. Dokumentasjonen viser at de fleste styringsdokumentene og rutinene er godkjent i 2025, noe som indikerer en pågående prosess for å styrke internkontrollen. Tiltak for å ivareta registrertes rettigheter er beskrevet, og det er etablert mekanismer for innsyn, samtykkehåndtering og sletting.

Samtidig fremkommer det flere svakheter. Intervjuer med ansatte og ledere viser at implementeringen av rutiner ikke er konsekvent, særlig ved oppgraderinger og utviklingsprosjekter. Det mangler risikovurderinger og DPIA for flere systemer. Kompetansenivået på personvern og informasjonssikkerhet blant systemeiere og ledere beskrives som utilstrekkelig, og rolleavklaringer mellom interne aktører og FRID IKS er uklare. Manglende oversikt over systemkritikalitet og fravær av rutiner for loggkontroller og stikkprøver forsterker risikoen. Kostnadsreduksjoner hos FRID trekkes frem som en faktor som svekker sikkerhetsnivået. Videre viser e-læringsstatistikken at kun 34 % av ansatte har gjennomført cybersikkerhetskurset i 2024, noe som indikerer begrenset opplæring og bevisstgjøring.

Det er gjennomført en gap-analyse mot ISO-standarder og NSMs grunnprinsipper, og det foreligger en tiltaksplan for lukking av avvik innen tredje kvartal 2026. Dette viser at fylkeskommunen har identifisert forbedringsområder og arbeider med å styrke internkontrollen, men flere tiltak er fortsatt under implementering.

Konklusjon

Undersøkelsen viser at Buskerud fylkeskommune i hovedsak har etablert et helhetlig rammeverk for internkontroll innen informasjonssikkerhet og personvern, med styringssystem, styrende dokumenter og operative rutiner som er i samsvar med gjeldende regelverk og anerkjente standarder. Mange styringsdokumentet foreligger og flere er under utarbeidelse. Dette viser at dette er et område fylkeskommunen har fokus på. Ledelsesforankringen er også tydelig, og det foreligger mekanismer for avvikshåndtering, risikovurdering og ivaretakelse av registrertes rettigheter.

Samtidig foreligger det vesentlige svakheter knyttet til implementering og etterlevelse. Manglende risikovurderinger og DPIA for flere systemer, uklare roller og ansvar, begrenset kompetanse og lav gjennomføring av opplæring svekker internkontrollens effektivitet. Det er også behov for bedre rutiner for

loggkontroller og systemkritikalitet, samt tydeligere involvering av personvernombudet i alle pålagte og relevante prosesser.

Fylkeskommunen har etablert nødvendige strukturer og dokumentasjon, men mangler konsekvent implementering og tilstrekkelig kompetanse for å sikre at internkontrollen fungerer som forutsatt. Tiltaksplanen og pågående forbedringsarbeid indikerer vilje til å lukke avvik, men per revisjonstidspunkt er flere kritiske elementer ikke fullt ut ivaretatt.

5. Personvern

Dette kapittelet setter søkelys på problemstilling 2:

Har fylkeskommunen sikret at det er etablert et tilfredsstillende vern av fysiske personer i forbindelse med behandling av personopplysninger?

Til denne problemstillingen har vi i kapittel 3 utledet følgende revisjonskriterier:

- Databehandleravtaler skal inngås når fylkeskommunen setter ut behandling av personopplysninger til en ekstern part (databehandler).
- Fylkeskommunen som behandlingsansvarlig skal påse at databehandler følger regelverket, herunder blant annet gjennomfører risikovurderinger og personkonsekvensvurdering der det behandles personopplysninger.
- Fylkeskommunen skal sikre at personvernombudet på riktig måte og i rett tid involveres i alle spørsmål som gjelder vern av personopplysninger

5.1. Fakta

Dokumentet "Rollebeskrivelse Personvernombud" beskriver rollen, arbeidsoppgaver og rammer for personvernombudet i fylkeskommunen. Personvernombudet fungerer som en uavhengig rådgiver for hele fylkeskommunens virksomhet, samt som ombud for innbyggere og ansatte med registrerte personopplysninger. Ombudet skal ikke instrueres i prioriteringer eller løsninger, og kan heller ikke tildeles oppgaver som utfordrer uavhengigheten.

Arbeidsoppgavene deles i innadrettede og utadrettede oppgaver. Internt skal ombudet informere og gi råd om personvernregelverket, delta i relevante prosesser, bistå med opplæring og kompetanseheving, kontrollere overholdelse av regelverk. Personvernombudet kan også bistå og konferere i arbeidet med behandlingsprotokoll, i utarbeidelsen av personvernkonsekvensvurderinger og avvikshåndtering, samt rapportere regelmessig til ledelsen. Eksternt skal ombudet være kontaktpunkt mot Datatilsynet, tilgjengelig for spørsmål fra ansatte og innbyggere, og representere fylkeskommunen i relevante personvernforum.

Personvernombudet skal involveres tidlig i prosesser som påvirker personvernet, og alle virksomheter skal legge til rette for samarbeid og informasjonsutveksling. Ombudet skal ha tilgang til nødvendig informasjon og systemer for å utføre sine oppgaver, og informeres om avvik som kan kreve melding til Datatilsynet.

Navn og kontaktinformasjon til personvernombudet skal være kjent for ansatte og innbyggere, og registreres hos Datatilsynet. Rapportering skjer årlig med en oppsummerende rapport til fylkeskommunedirektørens ledergruppe, halvårlig med status og vurderinger, samt løpende ved behov.

«Årsrapport 2024 fra personvernombudet» for Buskerud fylkeskommune tar utgangspunkt i personvernombudets arbeid og vurderinger på systemnivå i 2024, med særlig fokus på status, styring og kontroll av personvernområdet i fylkeskommunen. Personvernombudet har bistått med anbefalinger og støtte for å styrke systematikken i personvernarbeidet, fylkeskommunen har igangsatt viktige forbedringsprosjekter knyttet til organisering, styringssystem og avvikshåndtering. Det pekes på flere risikoområder, blant annet knyttet til ansvarlighetsprinsippet og outsourcing av tjenester til FRID IKS hvor det er behov for tydeligere rolle- og ansvarsfordeling, særlig når det gjelder databehandleravtaler, risikovurderinger og personvernkonsekvensvurderinger (DPIA).

Rapporten fremhever at fylkeskommunen har et stykke igjen for å oppfylle den lovpålagte rådføringsplikten med personvernombudet, og at ansatte i skolen fortsatt mangler et saks- og arkivsystem som ivaretar sikker deling og lagring av sensitive personopplysninger. Personvernombudet har hatt et konstruktivt samarbeid med ledelsen og har bidratt med kartlegging, anbefalinger, opplæring og deltakelse i relevante nettverk og konferanser.

Blant de viktigste forbedringene i 2024 nevnes organisatorisk plassering av ansvar for informasjonssikkerhet og personvern, rekruttering av ny ressurs med kompetanse på området, opprettelse av prosjektgruppe for styringssystem, og utvikling av nye rutiner for avvikshåndtering. Personvernombudet peker på at det fortsatt er risiko knyttet til manglende kompetanse, uklarhet i roller og ansvar, og manglende oversikt over vurderinger og beslutninger.

Videre anbefales det å etablere personvernkontakter i virksomhetsområdene, styrke samhandling mellom rådgivningstjenesten i FRID IKS og fylkeskommunen, og tydeliggjøre hvilke oppgaver som skal håndteres internt og eksternt. Det understrekes at fylkeskommunen må prioritere arbeidet med behandlingsprotokoll, risikovurderinger og databehandleravtaler, samt sikre at personvernombudet involveres tidlig og systematisk i relevante prosesser.

Rapporten konkluderer med at det er behov for økt modenhet, bedre rutiner og tydeligere ansvar på personvernområdet, og at dette krever langsiktig og systematisk innsats på tvers av virksomheten. Særlig fremheves behovet for sikre digitale løsninger for ansatte i skolen, og at risikovurderinger og DPIA må gjennomføres før nye systemer tas i bruk for å ivareta elevenes personvern og fylkeskommunens lovpålagte ansvar.

Fylkeskommunen har lagt ved to databehandleravtaler inngått med henholdsvis FRID IKS og Visma.

Innsendt dokumentasjon viser at fylkeskommunen har gjennomført ROS-analyse for systemene Digital innsikt, Elements. FINT og Rayvn. Det foreligger også DPIA for Digital innsikt.

Intervjuer

I intervjuer med ansatte og ledere fremkommer det at fylkeskommunen står overfor betydelige utfordringer knyttet til personvern og informasjonssikkerhet. Det er avdekket mangler i gjennomføringen av ROS-analyser og personvernkonsekvensvurderinger (DPIA) for flere systemer, særlig de som er videreført fra Viken. Tidligere vurderinger er i liten grad dokumentert, og det finnes ikke en samlet oversikt over hvilke systemer det gjelder. Dette har ført til behov for en systematisk gjennomgang og oppdatering av risikovurderinger for å sikre etterlevelse av regelverket. Personvernombudet har påpekt at involvering skjer for sent i prosesser, ofte etter at systemer er anskaffet eller endringer implementert. Selv om det finnes rutiner for nyanskaffelser, mangler det faste prosedyrer for oppgraderinger og utviklingsprosjekter. Personvernombudet etterlyser tydeligere ansvarslinjer og bedre rutiner for involvering i alle relevante prosesser.

Det blir sagt at når det gjelder databehandleravtaler, inngås disse av FRID på vegne av fylkeskommunen, men det juridiske ansvaret ligger hos fylkeskommunen. Det er etablert rutiner som dekker hele prosessen fra kravspesifikasjon med personvernkrav, via tilbudsvurdering, risikovurdering og DPIA, til signering av avtale. FRID bistår også med kvalitetssikring av innholdet i nye avtaler og gjennomgang av eksisterende avtaler. Samtidig opplyses det om behov for tydeligere definering av roller og fullmakter, da uklarhet om FRIDs ansvar og fylkeskommunens oppfølging skaper risiko. Manglende risikovurderinger av leverandører og fravær av gyldige databehandleravtaler opplyses å kunne medføre alvorlige konsekvenser som manglende garanti for sikkerhetstiltak og risiko for ulovlig lagring av data i tredjeland.

Det kommer frem i intervjuene at det er igangsatt arbeid med å etablere styringssystem og rutiner for gjennomføring og lagring av ROS-analyser, DPIA og databehandleravtaler, samt kontrollrutiner for tilgang og logger. Prosjektet omfatter utarbeidelse av styringsdokumenter og implementering i organisasjonen, men manglende kompetanse og ressurser har forsinket fremdriften. Det arbeides nå med å definere tydelige roller og ansvar, samt å styrke samarbeidet med personvernombudet, som har deltatt i arbeidsgrupper og rådgitt i utvikling av rutiner for anskaffelser.

Det blir sagt at avvikshåndtering er etablert, personvernombudet får kopi av avviksmeldinger og tilbyr bistand ved behov. Rapportering har økt etter innføring av nye rutiner, men det antas fortsatt å være mørketall. Det mangler et godt system for å trekke ut styringsdata og analysere avvik på tvers av systemer. Kompetansenivået på personvern og informasjonssikkerhet er generelt lavt, og opplæring skjer hovedsakelig gjennom håndtering av enkeltavvik. Det finnes ikke et systematisk opplæringsprogram, noe som er identifisert som et forbedringspunkt.

Det fremkommer i intervjuer at planlagte forbedringer inkluderer etablering av en digitaliseringsstrategi, styrking av internkontroll og implementering av styringssystem for informasjonssikkerhet og personvern. Det er også ansatt en ny rådgiver med ansvar for informasjonssikkerhet som skal bidra til oppfølging og videreutvikling av styringssystemet. Tiltaksplaner er utarbeidet basert på risikovurderinger, arbeidet med å definere roller, kritikalitetsvurdering og tjenesteavtaler med leverandøren vil fortsette inn i 2026.

I intervju fremkommer det også at i ett tilfelle der sensitive personopplysninger fortsatt oppbevares fysisk i permer i et låst rom, uten krysslister og kontrolltiltak.

Intervju med Direktør for kommunikasjon, sikkerhet og myndighetskontakt og Fagansvarlig Informasjonssikkerhet og personvern

Fylkeskommunen har igangsatt arbeid med egne risikovurderinger og personvernkonsekvensvurderinger (DPIA), men har ikke full oversikt over tidligere vurderinger fra Viken. Det er usikkerhet om hva som er overlevert fra FRID IKS, dokumentasjonen anses som mangelfull. Fagansvarlig Informasjonssikkerhet og personvern har ansvar for å etablere tekniske risikovurderinger og DPIA-er inkludert kartlegging av systemeiere og innkjøpsprosesser. Det er også behov for tydeliggjøring av roller som tjenesteeier og behovseier, da det er ulik forståelse i organisasjonen for hva disse innebærer. Tjenesteeier skal definere krav til informasjonssikkerhet og tilgangsstyring, men kompetansen varierer og det er behov for felles begrepsbruk og struktur.

Når det gjelder strategisk arbeid har Buskerud fylkeskommune selv vurdert å ligge på digitaliseringstrinn 2,5. Fagansvarlig Informasjonssikkerhet og personvern planlegger en modenhetsvurdering og gap-analyse som skal presenteres for strategisk ledergruppe. Det foreligger ingen felles digitaliseringsstrategi, men det anses som hensiktsmessig å utarbeide en strategi for alle tre fylkeskommuner for å sikre effektiv bruk av FRID. Dokumentasjonen er begrenset, kvalitetssystemet brukes ulikt, noe som gjør det vanskelig å få oversikt. Det vurderes som et godt tiltak å anskaffe en egen løsning for styringssystemet for informasjonssikkerhet.

5.2. Revisjonens vurdering og konklusjon

Revisjonskriteriene stiller krav om at fylkeskommunen skal inngå databehandleravtaler ved utsetting av behandling av personopplysninger, gjennomføre risikovurderinger og personvernkonsekvensvurderinger (DPIA) der det behandles personopplysninger, samt sikre at personvernombudet involveres på riktig måte og i rett tid i alle spørsmål som gjelder vern av personopplysninger. Videre skal fylkeskommunen ha etablert internkontroll for arbeidet med personopplysninger og personvernombudets rolle.

Gjennomgangen viser at fylkeskommunen har etablert enkelte rutiner og dokumentasjon som dekker deler av kravene. Det foreligger databehandleravtaler med FRID IKS og Visma, og det er gjennomført ROS-analyser for flere systemer samt DPIA for Digital innsikt. Dette indikerer at fylkeskommunen har igangsatt arbeid for å oppfylle kravene til risikovurdering og avtaleinngåelse. Samtidig fremkommer det at gjennomføringen er ufullstendig og lite systematisk. Flere systemer mangler oppdaterte risikovurderinger og DPIA, særlig de som er videreført fra Viken, det finnes ikke en samlet oversikt over tidligere vurderinger. Dette innebærer at fylkeskommunen ikke fullt ut oppfyller kravet om å sikre etterlevelse av regelverket.

Når det gjelder involvering av personvernombudet, viser dokumentasjonen og intervjuene at ombudet har en tydelig rollebeskrivelse og deltar i relevante prosesser, men involvering skjer ofte for sent og etter at systemer er anskaffet eller endringer implementert. Dette er i strid med kravet om tidlig og systematisk involvering. Personvernombudet har imidlertid bidratt med rådgivning, opplæring og rapportering, og fylkeskommunen har lagt til rette for samarbeid gjennom etablerte rutiner for avvikshåndtering og rapportering. Det er likevel behov for bedre prosedyrer for oppgraderinger og utviklingsprosjekter, samt tydeligere ansvarslinjer.

Internkontrollen på personvernområdet er under utvikling. Det er igangsatt arbeid med styringssystem, rutiner for ROS-analyser, DPIA og databehandleravtaler, samt kontrollrutiner for tilgang og logger. Tiltaksplaner er utarbeidet, og en ny rådgiver er ansatt for å styrke kompetansen. Likevel er internkontrollen ikke fullt ut implementert, og det mangler systematisk opplæring og oversikt over vurderinger og beslutninger. Dette medfører risiko for manglende etterlevelse og svekket styring.

Revisjonens samlede vurdering er at fylkeskommunen har tatt viktige skritt for å etablere rutiner og styringssystemer, men at det fortsatt er betydelige mangler knyttet til systematikk, kompetanse og involvering av personvernombudet. Kravene til databehandleravtaler er delvis oppfylt, men det er behov for tydeligere rolle- og ansvarsfordeling og bedre oppfølging av leverandører.

Revisjonen vil også vise til at undersøkelsen avdekket at sensitive personopplysninger fortsatt oppbevares fysisk i permer i låste rom, uten krysselister og kontrolltiltak. Videre er det uklart om det foreligger ROS-analyse og DPIA for systemet som registrerer reiser med TT-kort. Systemet slik det er forklart for revisjonen kan være i strid med personopplysingsloven og GDPR. Det er ingen som har kunnet vise til risikovurderinger, og at det er et rettslig grunnlag for lagring av personopplysninger. Det faktum at de relevante personene i fylkeskommunen ikke er kjent med disse problemstillingene, indikerer manglende oversikt.

Konklusjon

Undersøkelsen viser at det er etablert databehandleravtaler og gjennomført enkelte risikovurderinger og DPIA, personvernombudet har en definert rolle og deltar i prosesser. Samtidig foreligger det vesentlige

avvik fra kravene om systematisk gjennomføring av risikovurderinger og DPIA og tidlig involvering av personvernombudet. Manglende oversikt, utydelige ansvarslinjer og lav kompetanse på området viser at arbeidet som gjøres ikke er tilstrekkelig og i samsvar med gjeldende regelverk. Revisjonens funn viser at fylkeskommunen har igangsatt forbedringer, men at det kreves langsiktig og systematisk innsats for å oppfylle lovpålagte krav og sikre et forsvarlig personvernarbeid.

6. Anbefalinger

Med bakgrunn i vår gjennomgang vil vi anbefale Buskerud fylkeskommune følgende:

- sikre at det etableres en tilstrekkelig internkontroll for arbeidet med informasjonssikkerhet og personvern.
- sikre implementering av internkontrollen for arbeidet med informasjonssikkerhet og personvern.
- sørge for at det utarbeides databehandleravtaler der det er påkrevd.
- sørge for at det utarbeides ROS-analyser og personvernkonsekvensvurderinger der det foreligger lovkrav om det.
- sørge for at personvernombudet blir involvert til rett tid i alle spørsmål som gjelder pålagte og relevante prosesser knyttet til personopplysninger.

Et utkast til rapport har blitt oversendt Fylkeskommunedirektøren til uttalelse. Fylkeskommunedirektørens uttalelse er vedlagt rapporten.

Drammen, den 15. januar 2026

Torkild Halvorsen	Ann Heidi Jebsen	Even Tveter
Oppdragsansvarlig	Prosjektleder	Prosjektmedarbeider

Referanser

Lov og forskrift:

- LOV 2018-06-22 nr 83 – Lov om kommuner og fylkeskommuner (kommuneloven)
- LOV 2018-12-20 nr 116, Lov om behandling av personopplysninger (personopplysningsloven)
- EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning)

Sentrale føringer:

- Prop. 56 LS (2017–2018), Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen
- Veiledere fra Datatilsynet
- Veiledere fra KINS – Foreningen kommunal informasjonssikkerhet

Lokale føringer:

- Fylkeskommunale vedtak, rutiner og retningslinjer

Vedlegg 1 – Uttalelse fra Fylkeskommunedirektør

Buskerud fylkeskommune

Uttalelse fra fylkeskommunedirektøren på rapport om forvaltningsrevisjon informasjonssikkerhet og personvern.

Buskerud fylkeskommune mottok rapporten 16.12.2025 med anmodning om å gi fylkeskommunedirektørens uttalelse innen 09.01.2026.

Overordnet vurdering

Buskerud fylkeskommune er i en oppbyggingsfase etter omorganisering og etablering som ny fylkeskommune 1. januar 2024. Sentrale strukturer for digitalisering, styring og internkontroll har derfor måttet etableres og forankres på nytt. Som del av dette arbeidet ble det i 2025 etablert en egen enhet for sikkerhet og beredskap, og det er ansatt en fagansvarlig for informasjonssikkerhet og personvern i full stilling. Dette har styrket både kapasitet og kompetanse på området.

Revisjonen viser at Buskerud fylkeskommune har etablert et strukturert rammeverk for arbeidet med informasjonssikkerhet og behandling av personopplysninger. Arbeidet er forankret i virksomhetens kvalitetssystem og består av sentrale styringsdokumenter, rutiner og rollebeskrivelser som samlet beskriver hvordan området er organisert, styrt og fulgt opp i tråd med gjeldende regelverk. Personvernombudets rolle er tydelig definert, med uavhengighet, rapportering og mandat som rådgiver og kontaktpunkt.

Samtidig viser revisjonen at internkontrollen mot informasjonssikkerhet og personvern ennå ikke fungerer fullt ut etter intensjonen i hele organisasjonen. Fylkeskommunedirektøren er enig i at dette gjelder implementering, systematikk, rolleavklaringer og kompetanse i linjen.

Revisjonens funn samsvarer med Buskerud fylkeskommune sine egne vurderinger, blant annet gjennom gjennomført i en intern gap-analyse og ekstern evaluering av oppgave- og ansvarsdeling mellom FRID IKS og eierfylkene.

Samlet vurdering av forvaltningsrevisjonen for informasjonssikkerhet og personvern

Fylkeskommunedirektøren deler revisjonens hovedbilde av at det foreligger sentrale styringsdokumenter og rutiner som dekker kjerneområder innen både informasjonssikkerhet og behandling av personopplysninger, herunder avvikshåndtering, risikovurderinger, behandlingsprotokoller, personvernkonsekvensvurderinger (DPIA), anskaffelser og leverandørforhold hvor hoveddelen av dokumentasjonen er formalisert i 2025.

Revisjonen viser at det fortsatt er behov for å styrke den praktiske etterlevelsen innen informasjonssikkerhet og personvern. Fylkeskommunedirektøren deler denne vurderingen, og det er identifisert forbedringstiltak gjennom risikovurdering av personvern, GAP-analyse mot relevante standarder og nasjonale grunnprinsipper, og helhetlig risiko- og sårbarhetsanalyse (HROS) innen sikkerhet og beredskap.

Buskerud fylkeskommune

Buskerud fylkeskommune har derfor allerede igangsatt og planlagt målrettede tiltak for å møte identifiserte forbedringsområder, blant annet knyttet til:

- fullføring og systematisering av risikovurderinger og DPIA for alle relevante systemer, inkludert systemer videreført fra tidligere organisering der dokumentasjonen er mangelfull, samt etablering av bedre struktur og samlet oversikt over systemer, systemeierskap og databehandleravtaler.
- bedre samlet og sporbar oversikt over vurderinger, beslutninger og behandlingsgrunnlag, støttet av videreutvikling av styringsdokumenter og styringsinformasjon.
- tydeligere rolle- og ansvarsavklaringer, inkludert grensesnittet mellom interne funksjoner og ekstern tjenesteleverandør, samt styrket porteføljestyring
- styrket oversikt over systemkritikalitet og mer systematiske kontroll- og oppfølgingsrutiner, herunder videreutvikling av avvikshåndtering
- økt kompetanse gjennom målrettet, obligatorisk opplæring og bevisstgjøring for ledere, systemeiere og nøkkelroller, som bidrar til forankring og kommunikasjon av styringsdokumenter og rutiner.
- tidligere og mer systematisk involvering av fagansvarlig informasjonssikkerhet og personvern, samt personvernombudet, gjennom tydeligere prosesskrav
- gjennomført gap-analyse, med dokumenterte tiltak, ansvar og tidsplan
- forbedre avviksløsning for å håndtere eventuelle avvik mer effektivt

Som et ledd i den videre modningen av området er det planlagt å etablere et helhetlig styringssystem for informasjonssikkerhet og personvern (ISMS) tidlig i 2027. Dette vil samle eksisterende rammeverk og praksis i ett system og bidra til økt struktur, styring og etterprøvbarhet og gjøre informasjonssikkerhet og personvern til en integrert del av virksomhetsstyringen.

Fylkeskommunedirektøren vil sikre at strategisk ledelse mottar samlet status og modenhetsvurderinger som grunnlag for prioritering og videre oppfølging, og at arbeidet inngår i ordinære styrings- og evalueringsprosesser.

Avslutning

Fylkeskommunedirektøren vurderer samlet sett at Buskerud fylkeskommune har lagt et nødvendig og godt fundament for arbeidet med informasjonssikkerhet og personvern.

Revisjonen bekrefter at retningen er riktig, samtidig som den tydeliggjør behovet for videre implementering og modning.

Med de tiltakene som er igangsatt og planlagt, og med etablering av et helhetlig ISMS som neste steg, legger fylkeskommunedirektøren til grunn at internkontrollen mot informasjonssikkerhet og personvern vil bli ytterligere styrket og bidra til trygg, lovmessig og tillitsskapende forvaltning i årene som kommer.

Vi kan kommuner

Viken kommunerevisjon IKS
Org.nr.: 985 731 098 MVA
post@vkrevisjon.no | vkrevisjon.no

Hovedkontor - Drammen
Postadresse: Postboks 4197, 3005 Drammen
Besøksadresse: Øvre Eiker vei 14, 3048 Drammen

Avdelingskontor - Hønefoss
Postadresse: Postboks 123, Sentrum, 3502 Hønefoss
Besøksadresse: Osloveien 1, 3511 Hønefoss

Avdelingskontor - Follo
Postadresse: Postboks 173, 1401 Ski
Besøksadresse: Parkaksen 7, 1400 Ski

Avdelingskontor - Hallingdal
Besøksadresse: Alfarvegen 117, 3540 Nesbyen