Revisjon Øst IKS

FORVALTNINGSREVISJONSRAPPORT

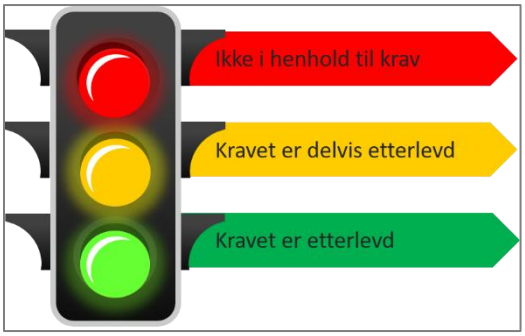
Digital sikkerhetskultur og personvern

STANGE KOMMUNE 2025

Postboks 84, 2341 Løten
Telefon: 62 43 58 00
https://www.revisjon-ost.no
E-post: post@rev-ost.no
Org. nr.: 974 644 576 MVA

Forord – om rapporten

Denne rapporten er bygget opp med et kort sammendrag som går gjennom hovedfunnene og konklusjonen i forvaltningsrevisjonsprosjektet i første kapittel.



Vi har valgt å benytte en «trafikklysmodell» for å illustrere hva vi mener er i henhold til krav på området, det som er godkjent med merknad, og det som ikke er i henhold til krav på området. Hver vurdering blir merket med henholdsvis grønt, gult og rødt.

Rapporten er utarbeidet med et digitalt tilsnitt og innehar lenker til ulike seksjoner av rapporten. Dette skal gjøre det enklere for leseren å navigere i rapportens innhold. Det er også lenket til de kilder som er digitalt tilgjengelige, for en mer interaktiv opplevelse av rapporten.

Rapporten er bygget opp etter NKRFs krav til sluttrapport i Standard for forvaltningsrevisjon (RSK 001). Dette innebærer minstekravene til

- sammendrag
- informasjon om bestillingen
- problemstillingene
- valg av metoder og vurdering av datagrunnlag
- revisjonskriterier (vedlegg A)
- presentasjon av data
- vurderinger
- konklusjon
- anbefalinger
- referanser
- kommunedirektørens uttalelse

I tråd med RSK 001, ønsker vi å fremheve at vi vektlegger at forvaltningsrevisjoner skal «bidra til et godt beslutningsgrunnlag for de folkevalgtes styring og kontroll, og å bidra til læring».

Vi vil takke kontrollutvalget for oppgaven, og administrasjonen for tilrettelegging for en best mulig og effektiv gjennomføring av forvaltningsrevisjonsprosjektet.

Vi håper at leseren finner nytte i rapporten og vil benytte denne videre i forbindelse med en trygg og god forvaltning av tjenesteområdet.

Kongsvinger, 18. august 2025

Kristin Fragell Lillevold
Oppdragsansvarlig forvaltningsrevisor

Eskil Kristiansen
Utøvende forvaltningsrevisor

Innholdsfortegnelse

Sammendrag

Formålet med forvaltningsrevisjonen har vært å undersøke om Stange kommune har en etablert digital sikkerhetskultur som ivaretar internkontroll og avvikshåndtering på en tilfredsstillende måte, samt undersøke i hvilken grad kommunen har rutiner og etablert praksis som sikrer at kommunen oppfyller sine plikter i henhold til personvernregelverket.

Forvaltningsrevisjonen har hatt følgende problemstillinger:

1. *Har Stange kommune etablert en god sikkerhetskultur i organisasjonen, herunder internkontroll og avvikshåndtering?*
2. *Har Stange kommune etablerte rutiner og praksis som sikrer et tilfredsstillende vern av fysiske personer i forbindelse med behandling av personopplysninger?*

I forbindelse med forvaltningsrevisjonen ble det gjennomført dokumentanalyse, intervjuer med ledere og nøkkelpersonell i kommunen, samt en spørreundersøkelse blant alle ansatte med minst 50 % stilling. Datainnsamlingen ble gjennomført i perioden januar til juni 2025.

Digital sikkerhetskultur og internkontroll på informasjonssikkerhetsområdet

Undersøkelsen viser at Stange kommune alt overveiende har etablert en god sikkerhetskultur i organisasjonen, herunder internkontroll og avvikshåndtering. Kommunen har en tilfredsstillende overordnet informasjonssikkerhetsstrategi samt en sikkerhetsorganisasjon med klare beskrivelser av roller og ansvar i informasjonssikkerhetsarbeidet. Kommunens internkontroll omfatter informasjonssikkerhet, og internkontrollsystemet for informasjonssikkerhet og personvern gjennomgås årlig for å sikre at det fungerer etter hensikten og blir videreutviklet. Kommunen har videre et tilfredsstillende avvikssystem og prosedyrer for håndtering og oppfølging av avvik på informasjonssikkerhetsområdet.

Undersøkelsen viser samtidig at kommunen har prosedyrer for å gi ansatte relevant opplæring i informasjonssikkerhet og personvern, men har likevel et forbedringspotensial med hensyn til å få ansatte til å gjennomføre slik opplæring. Resultatene fra spørreundersøkelsen indikerer at mange vurderer risikoen som lav, på områder det er knyttet høy risiko til. Samtidig er det en betydelig andel av de ansatte som ikke er kjent med virksomhetens regler for digital sikkerhet. Revisjonen vurderer at kommunen ikke fullt ut har etablert en god nok sikkerhetsatferd blant de ansatte i organisasjonen.

Revisjonen konkluderer at Stange kommune har etablert et rammeverk som tilrettelegger for god sikkerhetskultur, men at det er et forbedringspotensial knyttet til sikkerhetsatferden til de ansatte.

Overholdelse av personvernlovverket

Undersøkelsen viser at Stange kommune har etablert rutiner og praksis som sørger for at kommunen har tilgang på riktig kompetanse på personvernområdet og sikrer at enkeltpersoner får informasjon om kommunens behandling av personopplysninger. Kommunen ivaretar lovpålagte personvernombudstjenester og sørger for å involvere personvernombudet der det er relevant, og har utarbeidet en omfattende personvernerklæring som tilrettelegger for at den registrerte kan utøve sine rettigheter etter personvernlovgivningen.

Undersøkelsen viser også at kommunen ikke i tilstrekkelig grad har etablert praksis som sørger for tilfredsstillende gjennomføring av risikovurderinger på personvernområdet (DPIA), og når det gjelder å tydelig kommunisere hva som forventes av den enkelte ansatte med hensyn til digital sikkerhet.

Videre har ikke Stange kommune vært i stand til å legge frem gjeldende databehandleravtaler for alle sine systemer innen revisjonens frister, og dermed heller ikke behandlingsprotokoll knyttet til de samme systemene. Per august 2025 har revisjonen fått dokumentert at dette er kommet på plass, men for enkelte systemer er det usikkert om det har vært noen gjeldende databehandleravtaler før august 2025.

Informasjon vi har mottatt underveis i prosjektet tyder imidlertid på at det er flere prosesser i gang som vil svare ut forbedringspunktene og avvikene. De planlagte endringene i Indigo-samarbeidet vil blant annet innebære at Indigo-kommunene får et felles GDPR-system i forbindelse med innføring kvalitets- og internkontrollsystemet Samsvar. I Samsvar vil Indigo-kommunene blant annet kunne gjennomføre DPIA, samt samle alle databehandleravtaler på ett sted som vil kunne bidra til å gjøre arbeidet med databehandleravtaler mer oversiktlig.

Revisjonen konkluderer med at Stange kommune ikke i tilstrekkelig grad har etablerte rutiner og praksis som sikrer et tilfredsstillende personvern gjennom databehandleravtaler for alle systemer i undersøkelsesperioden.

Anbefalinger

På bakgrunn av den gjennomførte undersøkelsen anbefaler vi at kommunedirektøren med hensyn til digital sikkerhetskultur og internkontroll bør:

- Sikre at ansatte i større grad gjennomfører kommunens opplæringstiltak på informasjonssikkerhetsområdet.

Og med hensyn til etterlevelse av personvernlovverket anbefaler vi at kommunedirektøren må:

- Sørge for at risikovurderinger av personvernkonsekvenser (DPIA) gjennomføres i henhold til kommunens egne prosedyrer.
- Sørge for at kommunen og kommunens databehandlere systematisk fører protokoll over alle behandlingsaktiviteter.
- Sørge at kommunen har systematiske rutiner for å sikre at det foreligger gjeldende databehandleravtaler knyttet til alle kommunens systemer.
- Sikre at alle ansatte vet hva som forventes av dem med hensyn til digital sikkerhet.

Kommunedirektørens uttalelse

Et utkast til rapporten ble forelagt kommunedirektøren til uttalelse 11. juli 2025. I rapportutkastet var revisjonskriterie 11 og 13 vurdert til rødt på bakgrunn av at kommunen ikke hadde oversendt alle databehandleravtaler som revisjonen hadde bestilt. Underveis i høringsdialogen fikk revisjonen oversendt en ny databehandleravtale mellom Stange kommune og Visma Flyt AS. Revisjonen innarbeidet den nye databehandleravtalen i rapporten, og dette førte til at revisjonskriterie 11 og 13 ble endret til gult.

Kommunedirektøren fikk deretter forelagt et oppdatert utkast til rapporten til uttalelse 11. august 2025. Høringssvaret ble mottatt 18. august 2025. I høringssvaret beskriver kommunedirektøren at rapporten peker på nyttige læringspunkter som vil følges opp i kommunens forbedringsarbeid. Videre skriver kommunedirektøren at det i løpet av høsten 2025 vil iverksettes tiltak rettet mot å bedre

forbedringspunktene påpekt i rapporten. Samt at innføringen av Samsvar gjennom Indigo-samarbeidet vil gjøre kommunen bedre i stand til å gjennomføre systematiske aktiviteter og holde oversikt over dokumentasjon på personvernområdet.

Kommunedirektørens uttalelse er i sin helhet gjengitt i kapittel 7.

1 Innledning

1.1 Bakgrunn for prosjektet

Det følger av kommuneloven § 23-2, punkt c, at kontrollutvalget skal påse at det blir gjennomført forvaltningsrevisjon i kommunen. Forvaltningsrevisjon innebærer å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak, jf. kommuneloven § 23-3, første ledd.

Kontrollutvalget i Stange kommune behandlet prosjektplan om digital sikkerhetskultur og personvern i møte den 14. oktober 2024 (sak 45/24). På bakgrunn av prosjektplanens forslag til formål og problemstillinger, fattet kontrollutvalget følgende vedtak:

Vedtak, enstemmig:
Kontrollutvalget godkjenner revisors prosjektplan innen forvaltningsrevisjon av personvern og IKT under følgende forutsetninger:

a) *Kontrollutvalgets merknader og innspill som fremkom i møte tas med i det videre arbeidet.*
b) *Kommunestyrets godkjennelse av kontrollutvalgets plan for forvaltningsrevisjon og eierskapskontroll i kommunestyrets møte 23. oktober 2024.*

Kontrollutvalgets innspill til prosjektplanen omhandlet avvikskultur og sikkerhetsdefinisjoner, nærmere bestemt om det er en felles forståelse for avvik i organisasjonen og om kommuneledelsen har kommunisert felles sikkerhetsdefinisjoner nedover i organisasjonen slik at alle ansatte forstår sikkerhet på samme måte. Begge innspillene er hensyntatt i denne undersøkelsen.

I møte den 23. oktober 2024 vedtok kommunestyret kontrollutvalgets plan for forvaltningsrevisjon og eierskapskontroll for Stange kommune 2024-2028, jf. sak 81/24.

1.2 Formål og problemstillinger

Formålet med forvaltningsrevisjonen har vært å undersøke om Stange kommune har en etablert digital sikkerhetskultur som ivaretar internkontroll og avvikshåndtering på en tilfredsstillende måte, samt å undersøke i hvilken grad kommunen har rutiner og etablert praksis som sikrer at kommunen oppfyller sine plikter i henhold til personvernregelverket.

Formålet er belyst gjennom å besvare følgende problemstillinger:

1. Har Stange kommune etablert en god sikkerhetskultur i organisasjonen, herunder internkontroll og avvikshåndtering?
2. Har Stange kommune etablerte rutiner og praksis som sikrer et tilfredsstillende vern av fysiske personer i forbindelse med behandling av personopplysninger?

1.3 Indigo-samarbeidet

Indigo IKT er et interkommunalt IKT-selskap som drifter, forvalter, og utvikler løsninger for ni eierkommuner i Innlandet, deriblant Stange kommune. Indigo IKT er kommunens premissleverandør for IT-sikkerhet og er en sentral aktør i tematikken for denne forvaltningsrevisjonen, og mye av kommunens informasjonssikkerhetsarbeid blir utført i samarbeid med selskapet eller de andre kommunene i Indigo-samarbeidet.

I oppstartsmøtet med kommunen ble revisjonen gjort oppmerksomme på noen store endringsprosesser i regi av Indigo-samarbeidet som direkte berører kommunens arbeid med

informasjonssikkerhet og personvern. Nærmere bestemt dreier dette seg om to overordnede prosesser:

- Felles ISMS-system [1]
    - I praksis vil dette innebære at alle policy-dokumenter knyttet til informasjonssikkerhetsarbeid i eierkommunene samles og holdes oppdatert i Indigo IKT sitt kvalitetssystem. Deretter kan eierkommunene hente ut de oppdaterte dokumentene og laste de opp i sine egne kvalitetssystemer.
- Felles GDPR-system [2]
    - All dokumentasjon knyttet til personvernarbeid i Indigo-kommunene skal samles i Samsvar, som er et skybasert kvalitets- og internkontrollsystemet. Samsvar skal også være driftsrigg for alle fagsystemer. Dette innebærer også at alle risikovurderinger som ROS-analyser og personvernskonsekvensvurderinger (DPIA) skal utføres i Samsvar.

I rapporten henvises det til disse endringsprosessene der det er relevant. Per 8. juli 2025 er ikke disse endringsprosessene avsluttet enda.

1.4 Justeringer

Underveis i arbeidet med prosjektet ble det tydelig at de krav og forventninger vi hadde tillagt revisjonskriterie 14 (se Vedlegg A) ble besvart under revisjonskriteriene 4, 6, og 8. Vi valgte derfor å fjerne det som opprinnelig var revisjonskriterie 14, og som omhandlet kompetanse i organisasjonen og gjennomføring av risikovurderinger.

1.5 Leseveiledning

For å gi leseren en bedre forståelse av rapportens tematikk har vi utarbeidet en liste med begreper og forkortelser vi mener det er nyttig for leseren å ha oversikt over når man leser rapporten.

Begrep / Forkortelse	Forklaring
Sikkerhetskultur	Summen at de ansattes felles forståelse, holdninger, og praksis knyttet til informasjonssikkerhet, særlig hvordan de forholder seg til risiko, regler, og sikkerhetsrutiner
Informasjonssikkerhet	Handler om å beskytte all informasjon mot uautorisert tilgang, endring, eller ødeleggelse
Personvern	Handler om individets rett til å kontrollere egne personopplysninger og hvordan disse samles inn, brukes, og deles
EQS	Kommunens kvalitetssystem
DPIA	Vurdering av personvernkonsekvenser. Virksomheter har plikt til å vurdere personvernkonsekvensene i ulike løsninger de tar i bruk
Samsvar	Et skybasert kvalitets- og internkontrollsystem som kan bygges opp av ulike moduler etter virksomhetens behov.
RSO-analyse	Avgrensede konsekvensvurderinger av et tjenesteområde, et system, en teknisk komponent eller teknisk infrastruktur. Kommunen skal gjennomføre slike analyser på alt som har med personvern å gjøre
Behandlinger	I personvernsammenheng menes enhver bruk av personopplysninger

[1] Information Security Management System (ISMS) er et styringssystem for informasjonssikkerhet.

[2] General Data Protection Regulation (GDPR) kalt Personvernforordningen på norsk ble innført i 2018 og gir en enhetlig og streng regulering for personvern i Europa. Formålet er å gi enkeltpersoner kontroll over sine egne personopplysninger, samt å regulere hvordan virksomheter samler inn og bruker personopplysninger.

Behandling/ behandlingsprotokoll	Alle behandlingsansvarlige (som en kommune) skal føre protokoll over behandlingsaktiviteter som utføres under deres ansvar. Lovverket definerer hva behandlingsprotokoller skal inneholde
ESA	Kommunens sak- og arkivsystem. Systemet er i ferd med å fases ut og blir erstattet av sak og arkivsystemet Elements i november 2025. Elements er en videreutvikling av blant annet ESA
«De registrerte»	«Den registrerte» refererer til en person som kan identifiseres, direkte eller indirekte, gjennom innsamlede personopplysninger. Med andre ord er «de registrerte» i denne sammenhengen alle personer hvis personopplysninger er blitt innsamlet og behandlet av kommunen eller på vegne av kommunen

2 Metode for revisjonen

Forvaltningsrevisjonsprosjektet er gjennomført i henhold til NKRF sin Standard for Forvaltningsrevisjon, RSK001. Det følger av standarden at problemstillingene i prosjektet er bestemmende for valg av metode ved innsamling av data.

I henhold til standarden skal revisor innhente data i tilstrekkelig omfang til å kunne besvare prosjektets problemstillinger og å gjøre velbegrunnede vurderinger. Vi har derfor etterstrebet å benytte oss av metodetriangulering for å styrke rapportens reliabilitet og validitet, dette vil si å innhente data om samme forhold gjennom flere ulike metoder.

Vi har i denne undersøkelsen benyttet dokumentstudier, intervjuer, og spørreundersøkelse som metoder for innhenting av data. Datainnsamlingen ble gjennomført i perioden januar til juni 2025.

2.1 Dokumentstudier

Skriftlig dokumentasjon er en viktig kilde til informasjon om kommunens rutiner og praksis. Dokumentstudier innebærer gjennomgang og vurdering av relevant dokumentasjon opp mot fastsatte revisjonskriterier.

Den 27. januar 2025 ble det foretatt en dokumentbestilling. I tillegg har det blitt samlet inn dokumenter i forbindelse med intervjuer når det er blitt nevnt dokumenter som har vært interessante i forhold til prosjektets tematikk. Sentrale dokumenter i prosjektet har vært strategiske plandokumenter, rutiner og prosedyrer, samt eksempler på gjennomførte risikovurderinger, databehandleravtaler, og behandlingsprotokoller. Alle dokumentene som er en del av datagrunnlaget i rapporten, er opplistet som referanser i kapittel 8.2.

2.2 Intervjuer

Det ble innledningsvis gjennomført et oppstartsmøte (16.12.24) der følgende deltakere fra kommunen var til stede:

- Kommunedirektør
- Enhetsleder for Digitalisering og utvikling (Fagansvarlig for informasjonssikkerhet og personvern, heretter benevnt «fagansvarlig»)

Formålet med møtet var å informere kommuneadministrasjonen om forvaltningsrevisjonsprosjektet, samt gi mulighet for spørsmål og innspill til undersøkelsens tema og innretning. Det ble skrevet referat fra oppstartsmøtet som i etterkant ble verifisert av møtedeltakerne.

Det er videre, i perioden mai til juni 2025, gjennomført intervjuer med utvalgte ansatte som har ansvar og oppgaver innenfor forvaltningsrevisjonens tematikk. Formålet med intervjuer er å belyse samme tema fra ulike sentrale aktørers perspektiv. Følgende personer i kommunens organisasjon er intervjuet:

- Kommunedirektør (avsluttende intervju)
- Enhetsleder for Digitalisering og utvikling (Fagansvarlig for informasjonssikkerhet og personvern)
- Kommunalsjef Oppvekst (Systemeier for Oppvekst)
- Kommunalsjef Helse (Systemeier for Helse og mestring)
- Virksomhetsleder Arkiv (Systemeier for arkivtjenesten)
- Rådgiver IKT Helse og mestring (Systemansvarlig for Helse og mestring)
- Arkivleder (Systemansvarlig for arkivtjenesten)

Systemeierne og de systemansvarlig ble utvalgt på bakgrunn av at revisjonen hadde plukket ut fagsystemene i virksomhetsområdene Oppvekst og Helse og mestring, samt i kommunens sak- og arkivsystem for nærmere undersøkelse.

I tillegg sendte vi en liste med spørsmål til kommunens personvernombud på epost som vedkommende ble bedt om å svare ut skriftlig.

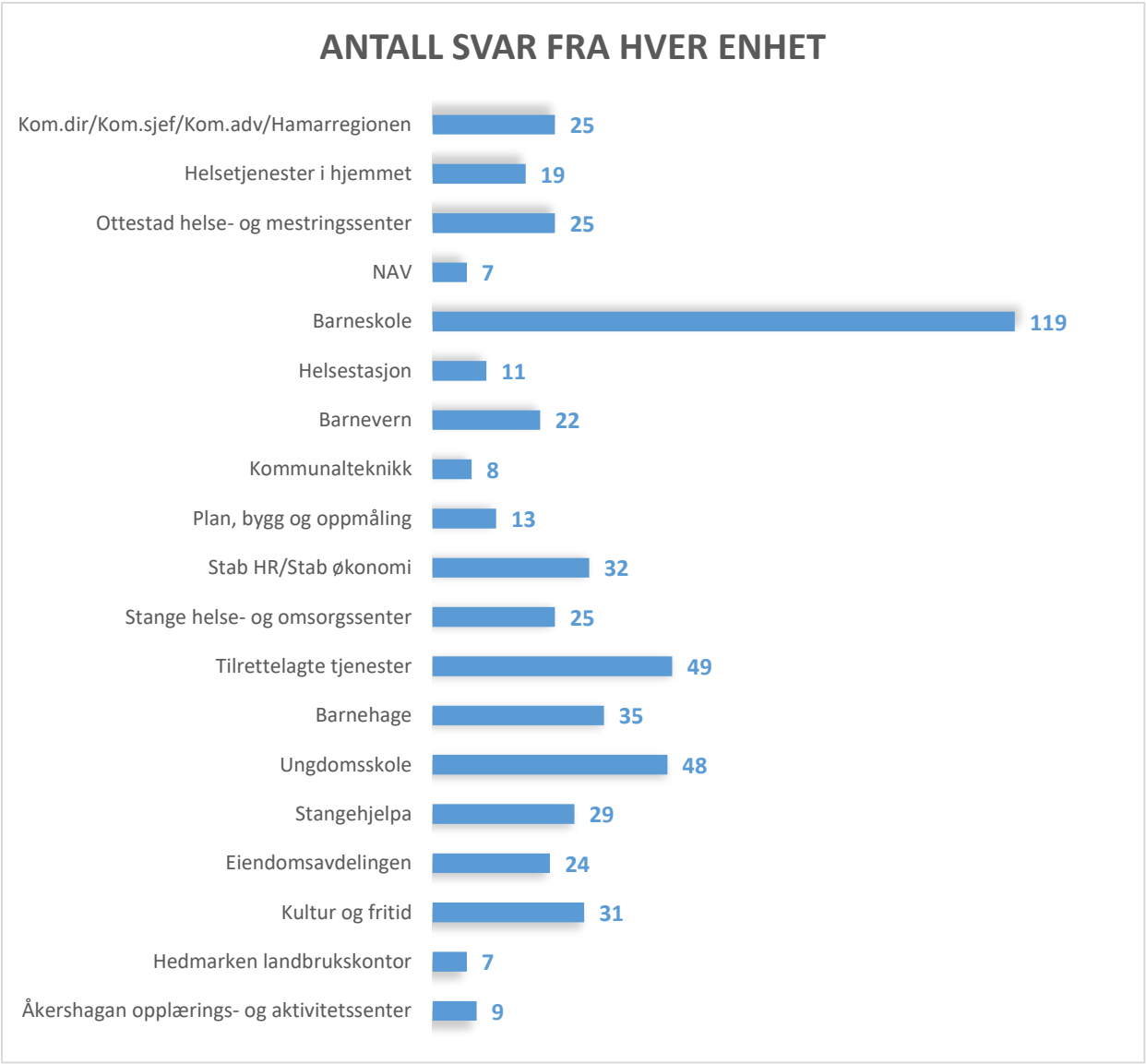
2.3 Spørreundersøkelse

Vi har gjennomført en spørreundersøkelse blant ansatte med minst 50 % stilling i Stange kommune.

Spørreundersøkelsen ble sendt ut 30. januar 2025 og levert til 1548 e-postadresser. Spørreundersøkelsen ble avsluttet 07. mars 2025. Svarprosenten på spørreundersøkelsen endte på 35, som vil si at 538 ansatte besvarte undersøkelsen. Svarprosenten for det enkelte spørsmål vil imidlertid variere, da noen respondenter ikke har besvart alle spørsmålene. Ingen av spørsmålene var obligatoriske. Revisjonens analyse av spørreundersøkelsesdataene finnes i Vedlegg B.

Innledningsvis inkluderte spørreundersøkelsen noen kategoriseringsspørsmål som gjorde at vi kunne gjennomføre krysstabuleringer [3] for å sammenligne svarene fra eksempelvis ansatte med eller uten lederansvar, og basert på hvor lenge de ansatte har arbeidet i kommunen. Respondentene fordelte seg på følgende enheter i kommunen:

[3] Krysstabulering vil si å sammenligne resultater fra forskjellige variabler. Man kan dermed sammenligne svarene på spesifikke spørsmål fra ulike respondentgrupper.



Kilde: Revisjon Øst, Questback N=538

Diagrammet viser at det er stor variasjon i hvor representert den enkelte enhet er i det totale svargrunnlaget i spørreundersøkelsen. Eksempelvis utgjør barnehageansatte over en femtedel av svarene, mens ansatte fra NAV eller Hedmarken landbrukskontor utgjør under 2 %. Variasjonen skyldtes både størrelsen på enhetene og svarprosenten blant ansatte innenfor hver av enhetene. I rapporten har vi skilt ut svarene fra den enkelte enhet der det er relevant.

Vi forsøkte å oppnå så høy svarprosent som mulig ved blant annet å forankre spørreundersøkelsen i kommunens ledelse, gjennom dialog med kommunedirektøren og enhetslederen for Digitalisering og utvikling. Kommunen sørget for at de ansatte ble informert om spørreundersøkelsen før invitasjonene ble sendt ut. I tillegg fikk de ansatte informasjon om formålet med undersøkelsen i eposten med invitasjonslenken, samt i innledningen til selve spørreskjemaet. Videre ble det sendt ut totalt seks automatiske påminnelser til de ansatte som ikke hadde besvart undersøkelsen, og perioden hvor spørreundersøkelsen var åpen for besvarelser ble utvidet med to uker på grunn av vinterferieavvikling.

For å sikre et representativt utvalg ble som nevnt undersøkelsen sendt til alle ansatte med minst 50 % stilling i kommunen, og invitasjonslenken ble sendt til epostadressen som er registrert på den enkelte ansatte for å sikre at alle fikk anledning til å besvare spørreundersøkelsen.

For å undersøke mulige skjevheter i utvalget er det i etterkant gjennomført en frafallsanalyse. Når vi ser på representasjon, så ser vi til andel svar innenfor en enhet i forhold til totale svar. Deretter sammenholder vi dette med hvor stor andel ansatte det er i enheten i forhold til antallet ansatte i kommunen med minst 50 % stilling. Vi får da et utgangspunkt for å kunne kontrollere for skjevheter i hvem som har besvart. Det handler med andre ord om proporsjonalitet. Mulige skjevheter vil omtales der dette er relevant i rapporten.

Frafallsanalyse					
Enhet	**Populasjon i enhet**	**Enhetens prosentandel av total populasjon**	**Antall svar**	**Svarprosent i enhet**	**Svarprosent i enhet ift., totalt antall svar**
Kom.dir/Kom.sjef/Kom.adv/Hamarregionen	45	3 %	25	56 %	5 %
Helsetjenester i hjemmet	135	9 %	19	14 %	4 %
Ottestad helse- og mestringssenter	73	5 %	25	34 %	5 %
NAV	28	2 %	7	25 %	1 %
Barneskole	278	18 %	119	43 %	22 %
Helsestasjon	22	1 %	11	50 %	2 %
Barnevern	34	2 %	22	65 %	4 %
Kommunalteknikk	11	1 %	8	73 %	2 %
Plan, bygg og oppmåling	18	1 %	13	72 %	2 %
Stab HR/Stab Økonomi	42	3 %	32	76 %	6 %
Stange helse- og omsorgssenter	131	9 %	25	19 %	5 %
Tilrettelagte tjenester	248	16 %	49	20 %	9 %
Barnehage	149	7 %	35	24 %	7 %
Ungdomsskole	112	7 %	48	43 %	9 %
Stangehjelpa	62	4 %	29	47 %	5 %
Eiendomsavdelingen	90	6 %	24	27 %	5 %
Kultur og fritid	62	4 %	31	50 %	6 %
Hedmarken landbrukskontor	8	1 %	7	88 %	1 %
Åkershagan opplærings- og aktivitetssenter	47	3 %	9	19 %	2 %
Totalt	**1548**		**538**		**100 %**

Kilde: Revisjon Øst, Questback

Frafallsanalysen viser at ansatte i deler av helsesektoren i kommunen er underrepresentert i spørreundersøkelsen. Svarprosenten fra helsetjenester i hjemmet, Stange helse- og omsorgssenter, og tilrettelagte tjenester utgjør til sammen 18 %, mens disse enhetenes populasjon utgjør 34 % av den

totale populasjonen i undersøkelsen. Dette svekker disse dataenes gyldighet og resultatene fra disse enhetene må tas med forbehold om man ser dem isolert.

Samtidig ser vi at flere enheter er overrepresentert, det vil si at svarprosenten til enheten av totalen er større enn enhetens andel av den totale populasjonen i undersøkelsen. Svarprosenten blant ansatte i barneskolen utgjør eksempelvis 22 % av alle svar, mens enhetens størrelse utgjør 18 % av den totale populasjonen. Flere andre mindre enheter er også overrepresentert. Dette styrker dataenes gyldighet.

I og med at data fra spørreundersøkelsen i all hovedsak viser til hva ansatte samlet sett har svart, mener vi totalt sett at antall svar og svarprosent på 35 gir viktig supplerende informasjon om aktuelle tema i undersøkelsen.

2.4 Vurdering av reliabilitet og validitet

Pålitelige data, eller det å sikre reliabilitet, ivaretas ved å være nøyaktig under innsamling og analyse av data, og innebærer at vi kan stole på at informasjonen er korrekt. Undersøkelser, målinger eller kartlegginger vil alltid inneholde risiko for feil, det vil si at de ikke er pålitelige. Det å innhente informasjon om samme forhold fra flere kilder er en teknikk for å øke påliteligheten (reliabiliteten). Kravet til gyldighet, eller validitet, innebærer at de dataene som samles inn skal være relevant for å besvare problemstillingene i undersøkelsen. Eksempelvis må revisor vurdere om han eller hun har snakket med de riktige informantene, stilt de riktige spørsmålene og innhentet riktige dokumenter.

En svakhet ved datamaterialet er at kommunen har mange ulike systemer som behandler personopplysninger og vi har ikke gjennomgått alle systemene, noe som kan ha svekket representativiteten Vi har prioritert å intervjue de personene som sitter med ansvar for de største fagsystemene i kommunen, samt de som vi antok har mest kunnskap om fagsystemene og bruker systemene i det daglige. To av intervjuobjektene [4] i undersøkelsen er ansvarlig for mange av kommunens systemer som behandler sensitive personopplysninger. Dette gjorde at vi kunne innhente informasjon også om kommunens andre fagsystemer som i utgangspunktet ikke var valgt ut for nærmere kontroll. Samlet sett mener revisjonen at rapporten bygger på pålitelige og gyldige data som gir et forsvarlig grunnlag for de vurderinger, konklusjoner, og anbefalinger vi har kommet med.

[4] Kommunalsjefen for Oppvekst og kommunalsjefen for Helse og mestring.

3 Problemstilling 1 – Sikkerhetskultur

Har Stange kommune etablert en god sikkerhetskultur i organisasjonen, herunder internkontroll og avvikshåndtering?

3.1 Revisjonskriterier for problemstilling 1

Punktene under er en oversikt over de kriteriene vi har benyttet for å besvare problemstillingen og våre vurderinger av disse. Kriteriene er gjengitt i kortform. For en full utledning av revisjonskriteriene, se vedlegg A. Tabellen er interaktiv, og leseren kan gå rett til den enkelte vurdering ved å trykke på det enkelte kriterier. Vurderingene er knyttet til de data som er samlet inn og som blir gjengitt i kapitlene nedenfor.

	Kriterium 1	Kommunen må ha utarbeidet sikkerhetsmål og en sikkerhetsstrategi, og strategien må være kjent for de ansatte.
	Kriterium 2	Kommunen må ha en sikkerhetsorganisasjon med beskrivelser av ansvar og roller for informasjonssikkerhet.
	Kriterium 3	Kommunen må ha skaffet oversikt over sentrale informasjonsverdier og hvor kritiske disse er for kommunens drift og tjenesteproduksjon.
	Kriterium 4	Kommunen må ha en internkontroll som omfatter informasjonssikkerhet og personvern, herunder etablere aktiviteter som sikrer at internkontrollen gjennomføres og fungerer som forutsatt.
	Kriterium 5	Systemet for internkontroll innen informasjonssikkerhet og personvern bør gjennomgås årlig.
	Kriterium 6	Kommunen må ha tiltak som sikrer at ansatte får opplæring knyttet til informasjonssikkerhet og personvern.
	Kriterium 7	Kommunen må ha et system for avviksregistrering innenfor informasjonssikkerhet og personvern.
	Kriterium 8	Avvik må gjennomgås, håndteres, og brukes for forbedring av prosedyrer og praksis i ivaretakelsen av informasjonssikkerhet og personvern.

3.2 Innhentet data: Overordnet styring (kriterier 1-3)

3.2.1 Sikkerhetsmål og sikkerhetsstrategi

I dokumentet *Sikkerhetsmål og sikkerhetsstrategier* (Stange kommune 2021) heter det at kommunen har følgende sikkerhetsmål:

«All informasjon som Stange kommune forvalter skal behandles etter gjeldende lovverk og på en måte som ivaretar krav til konfidensialitet, integritet, tilgjengelighet, åpenhet, lovlighet og dataminimering. Dette gjelder all informasjon; både det som finnes digitalt, på papir eller kommuniseres muntlig. Informasjonssikkerhet er en nødvendig faktor for at Stange kommune skal løse sine oppgaver og ha tillit hos innbyggerne.»

Kommunen har flere styringsdokumenter som beskriver at kommunens arbeid med informasjonssikkerhet skal forankres i øverste ledelse og inngå i ansvarsområdet en leder til enhver tid

har. [5] Videre har kommunen utarbeidet en tabell som bryter ned de ulike faktorene i det nevnte sikkerhetsmålet til operasjonelle tiltak:

Slik vil Stange kommune ha det	Slik gjør Stange kommune det
Håndtering av informasjon er effektiv og i samsvar med verdier samt gjeldende lover, regler og avtaler.	• Roller og oppgaver i sikkerhetsarbeidet er beskrevet, kjent og etterleves • Informasjonssikkerhet og innebygd personvern – både teknisk og organisatorisk ivaretas før personopplysninger blir behandlet
Informasjon kommer ikke på avveie (konfidensialitet).	• Taushetsplikten respekteres • Tilgang til informasjon er basert på tjenstlig behov • Ledere og medarbeidere har nødvendig kompetanse og gode holdninger
Informasjon er til å stole på: Den er korrekt, oppdatert og ikke manipulert (integritet).	Informasjon blir • bare produsert av de som har rett til det • ikke endret utilsiktet eller urettmessig • oppdatert så raskt som mulig
Informasjon er tilgjengelig for de som skal ha tilgang til den når de trenger det (tilgjengelighet).	• Tilgjengelige IKT-systemer med riktige tilganger • Riktige tilganger til papirbasert informasjon
Åpen om hvordan informasjon behandles (åpenhet).	• Informerer om hvordan personopplysninger behandles • Gir registerte innsyn i egne opplysninger • Gir mulighet til å rette, slette og flytte personopplysninger
Respekterer innbyggernes personvern og deres rettigheter.	• Vi kjenner til og etterlever våre plikter og retningslinjer. • Vi ivaretar innbyggernes rettigheter
God sikkerhetskultur.	• Bygger nødvendig kompetanse og sikkerhetsbevissthet blant alle medarbeidere
Arbeidet med informasjonssikkerhet gir kontinuerlig forbedring.	• Arbeidet med informasjonssikkerhet er en del av internkontrollen, og bygger på anerkjent standard for styringssystem for informasjonssikkerhet • Avdekker feil som oppstår og lærer av dem • Vurderer og dokumenterer risiko og gjør nødvendige tiltak
Vi behandler ikke mer personopplysninger enn nødvendig (Dataminimering).	• Vi innhenter, behandler og oppbevarer ikke mer personopplysninger enn nødvendig • Vi sikrer at vi ikke behandler personopplysninger ut over formål og lovlighet

Kilde: Stange kommune 2021

Som tabellen viser til skal for eksempel kommunen ivareta målet om håndtering av informasjon i samsvar med gjeldende lover og regler, ved at roller og oppgaver i sikkerhetsarbeidet er beskrevet, kjent og etterleves. Videre skal kommunen etterleve målet om konfidensialitet ved at tilgangen på informasjon baseres på tjenstlige behov. I tillegg skal kommunen ivareta en god sikkerhetskultur ved å bygge nødvendig kompetanse og sikkerhetsbevissthet blant alle medarbeidere.

[5] Disse dokumentene er som følger: «Sikkerhetsmål og sikkerhetsstrategi», «IKT-sikkerhetsledelse», «Informasjonssikkerhet og personvern – Opplæringsskriv», og «Roller, oppgaver og myndighet knyttet til personopplysningsloven».

Revisjonen har videre fått oversendt forsiden til den delen av kommunens kvalitetssystem (EQS) som omhandler informasjonssikkerhet:

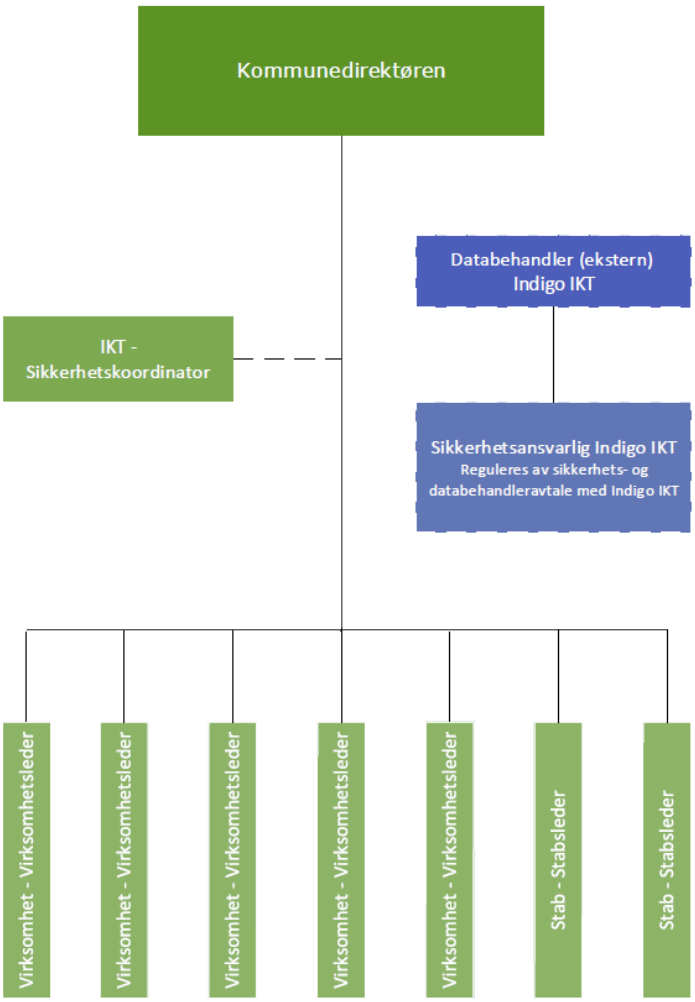
Kilde: Stange kommune 2025

Forsiden gir en oversikt over hva som er styrende (grønne), gjennomførende (gule), og kontrollerende (oransje) dokumenter for informasjonssikkerheten og personvern i kommunen. Fagansvarlig har forklart at ansatte kan klikke seg inn via forsiden i EQS på hver av bildene for å få mer informasjon om de enkelte temaene, deriblant om kommunens sikkerhetsstrategi. Kommunens sikkerhetsmål og personvernprinsippene som danner grunnlaget for sikkerhetsstrategien er også beskrevet i kommunens opplæringsskriv om informasjonssikkerhet og personvern. [6]

3.2.2 Sikkerhetsorganisasjon

Som beskrevet i kommunens sikkerhetsstrategi skal informasjonssikkerhet være forankret i kommunens øverste ledelse, samt være en del av ansvarsområdet en leder i kommunen har til enhver tid. [7] Revisjonen har fått oversendt et organisasjonskart som viser IKT-sikkerhetsledelsen i kommunen:

[6] Stange kommune (2025). *Informasjonssikkerhet og personvern - Opplæringsskriv*
[7] Stange kommune (2021). *Sikkerhetsmål og sikkerhetsstrategi*



Kilde: Stange kommune 2023

Av organisasjonskartet kan vi se at kommunedirektøren har det overordnede ansvaret for informasjonssikkerheten i kommunen, med hjelp av en IKT-sikkerhetskoordinator [8] samt Indigo IKT som kommunens premissleverandør for Stange kommunes IT-sikkerhet. Videre kan vi se at ansvaret for informasjonssikkerheten i kommunens ulike virksomheter er delegert til virksomhets- og stabslederne.

Ansvar, myndighet og oppgaver tillagt de ulike aktørene på informasjonssikkerhetsområdet, enten internt i kommunen eller som ivaretas av eksterne aktører, utgjør samlet viktige deler av internkontrollen, og er nærmere beskrevet i en egen oversikt kommunen har oversendt. [9]

Oversikten definerer blant annet at systemeiere har ansvar for å godkjenne risikovurderinger og vesentlige endringer i fagsystemer, samt har myndighet til å inngå og følge opp databehandleravtaler og serviceavtaler knyttet til drift og vedlikehold av fagsystemene. Daglig behandlingsansvar er lagt til avdelingsledere med personalansvar, mens systemansvarlige har ansvar for løpende kontakt med Indigo IKT og systemleverandør. Videre definerer oversikten at fagansvarlig har ansvar for at risikovurderinger er gjennomført og å holde oversikt over og følge opp kommunens databehandlere

[8] Denne rollen er endret navn til «fagansvarlig for informasjonssikkerhet og personvern».
[9] Stange kommune (2023). *Roller, oppgaver og myndighet knyttet til personopplysningsloven*

og systemleverandører med tanke på sikkerhet. I tillegg skal fagansvarlig sammen med personvernombudet bistå med fagkunnskap ved gjennomføring av DPIA. [10]

Oversikten definerer også hvilke ansvarsoppgaver kommunen forventer at eksterne aktører ivaretar i informasjonssikkerhetsarbeidet. Herunder skal Indigo IKT ha en aktiv rolle i kommunens informasjonssikkerhetsarbeid. Kommunens andre databehandlere skal følge den gjeldende databehandleravtalen samt fortløpende rapportere sikkerhetsavvik til kommunens fagansvarlig.

Kommunens internkontrollsystem beskrives ytterligere i kapittel 3.3.1.

3.2.3 Oversikt over sentrale informasjonsverdier

Oversikt over kommunens viktige informasjonsverdier med tilhørende kritikalitetsvurderinger foreligger i beredskapsplanen til Indigo IKT. I svar på dokumentbestillingen oppga fagansvarlig at informasjonsverdiene består av:

- AD-kontrollere [11]
- Nettverk og nettverkstjenester
- Databaser
- Hypervisior [12]
- Epostflyt
- Applikasjoner

Revisjonen har fått opplyst at som en del av de pågående endringsprosessene i Indigo-samarbeidet, er kommunen i ferd med å utarbeide en policy for klassifisering av informasjon.

3.3 Innhentet data: Internkontroll på informasjonssikkerhetsområdet (kriterie 4-6)

3.3.1 Internkontroll

I kommunens dokumenter [13] er det beskrevet at formålet med internkontroll på informasjonssikkerhet og personvern er å beskytte sensitive opplysninger og sikre at de behandles på en trygg og lovlig måte gjennom å:

- Sikre at informasjonen ikke kommer på avveie eller blir misbrukt
- Følge gjeldende lover og forskrifter, som personopplysningsloven og GDPR
- Forhindre uautorisert tilgang, hacking, og andre sikkerhetstrusler
- Bygge og opprettholde tillit blant innbyggerne ved å vise at kommunen tar informasjonssikkerhet og personvern på alvor
- Ha klare rutiner for hvordan man skal håndtere eventuelle sikkerhetsbrudd eller personvernbrudd

[10] Vurderinger av personvernkonsekvenser (*Data Protection Impact Assessment* - DPIA)
[11] Active Directory-kontrollere er servere som håndterer og sikrer tilganger til ressurser i et nettverk. Disse serverne verifiserer brukernavn og passord ved en innlogging, og sørger for at brukeren får tilgang til nettverksressurser som epost, filer, og applikasjoner.
[12] Hypervisior er en programvare som gjør det mulig å kjøre flere virtuelle maskiner på en fysisk maskin. Dette er sentralt innen IT-sikkerhet for å kunne isolere miljøer slik at man eksempelvis kan teste programvare uten risiko for hovedsystemet, hindre spredning av trusler, samt at det forenkler sikkerhetsgjenoppretting.
[13] Stange kommune (2025). *Informasjonssikkerhet og personvern - Opplæringsskriv*

Videre er det beskrevet at kommunen som behandlingsansvarlig sine daglige plikter ivaretas av virksomhetsledere som har fått delegert sin myndighet via respektiv kommunalsjef. Virksomhetslederne har i oppgave å:

- Sørge for at det er samsvar mellom gjeldende retningslinjer og praksis
- Iverksette tiltak på kort og lengre sikt for å forbedre personvernpraksisen
- Rette opp feil og mangler
- Sikre at alle som behandler personopplysninger har tilstrekkelig kompetanse og tilgang til nødvendig informasjon og dokumentasjon

Fagansvarlig har ansvar for å kontrollere at arbeidet utføres i henhold til bestemmelsene, og alle ansatte som behandler personopplysninger plikter å overholde bestemmelsene samt holde seg løpende orientert om lover og regler på området. På spørsmål om det er noen føringer på hvilke internkontrollaktiviteter på informasjonssikkerhetsområdet den enkelte virksomhetsleder skal utføre, forklarte kommunedirektøren i intervju at det er kommunens prosedyre med oversikt over roller, ansvar, og oppgaver på informasjonssikkerhetsområdet som legger rammene for dette. På bakgrunn av informasjon som kommer frem i kommunens dokumenter, [14] samt gjennom intervjuer, følger en oversikt over internkontrollaktiviteter på informasjonssikkerhetsområdet og hvilke ansatte som har ansvaret for å utføre disse:

- **Utarbeide beredskapsplan for informasjonssikkerhet**
  - Ansvar: Kommunedirektør
- **Holde prosedyrer knyttet til informasjonssikkerhet og personvern oppdatert**
  - Ansvar: Fagansvarlig
- **Ledelsens gjennomgang og systemrevisjon av informasjonssikkerheten**
  - Ansvar: Fagansvarlig
- **Gjennomføre tiltak vedtatt i ledelsens gjennomgang og systemrevisjon av informasjonssikkerheten i den enkelte virksomhet**
  - Ansvar: Systemeiere
- **Gjennomføre risikovurderinger (ROS-analyser) [15] ved innføring av nye systemer eller ved store systemendringer/oppgraderinger av eksisterende systemer**
  - Ansvar: Systemeiere med hjelp av fagansvarlig og sikkerhetsansvarlig i Indigo IKT ved behov
- **Tildeling, endring, og inndragning av tilganger**
  - Ansvar: Avdelingsledere (ledere med personalansvar)
- **Systematisk gjennomgang av logger iht., gjeldende rutiner**
  - Ansvar: Systemeiere i samarbeid med systemansvarlig
- **Gjennomføre opplæring av de ansatte om informasjonssikkerhet og personvern**
  - Ansvar: Avdelingsledere (ledere med personalansvar) og systemansvarlig med bistand fra fagansvarlig
- **Håndtere avvik innen informasjonssikkerhet**
  - Ansvar: Systemeiere, avdelingsledere (ledere med personalansvar), fagansvarlig, Indigo IKT, sikkerhetsansvarlig for Indigo IKT, og eksterne databehandlere. [16]

[14] Stange kommune (2023). *Roller, oppgaver og myndighet knyttet til personopplysningsloven*
[15] Risiko- og sårbarhetsanalyser.
[16] Hvem som er involvert i håndteringen av et avvik vil avhenge av avvikets art og omfang.

- **Gjennomføre vurdering av personvernkonsekvenser (DPIA)**
    - Ansvar: Systemeiere sammen med fagansvarlig og kommunens personvernombud
- **Utarbeide behandlingsprotokoller**
    - Ansvar: Avdelingsledere (ledere med personalansvar) i samarbeid med systemansvarlige og fagansvarlig

Oversikten over viser at ansvaret for å gjennomføre internkontrollaktivitetene på informasjonssikkerhetsområder er delegert nedover i kommunens organisasjon og ut i de ulike virksomhetene. I intervju spurte revisor hvordan kommunedirektøren blir holdt underrettet om internkontrollen. Kommunedirektøren forklarte at dette i hovedsak skjer gjennom fagansvarlig som deltar i ledermøter når informasjonssikkerhet er tema og gjennom løpende oppdateringer dersom det oppstår situasjoner.

Under går vi nærmere inn på enkelte av internkontrollaktivitetene på informasjonssikkerhetsområdet som er nevnt over. De øvrige internkontrollaktivitetene blir omtalt andre steder i rapporten.

Beredskap

Med hensyn til beredskap har Stange kommune utarbeidet en helhetlig ROS-analyse som utgangspunkt for det kommunale beredskapsarbeidet. [17] Bortfall av IKT, herunder hvordan dette vil påvirke ivaretakelsen av personvern, er en del av den helhetlige ROS-analysen og beredskapsarbeidet til kommunen. [18] I tillegg til dette har Indigo IKT en egen beredskapsplan spesifikt rettet mot IT-hendelser som omfatter alle eierkommunene, deriblant Stange kommune. Videre fortalte kommunedirektøren i intervju at kommunen har gjennomført øvelser knyttet til bortfall av strøm og nett, og hvilke konsekvenser dette vil ha for kommunens tjenesteproduksjon. Samtidig har Indigo IKT hatt noen mindre øvelser, og i sikkerhetsrådet i Indigo-samarbeidet diskuterer de hvordan de skal arbeide med beredskap på tvers av eierkommunene. I tillegg til dette er fagansvarlig i ferd med å utarbeide tiltakskort [19] i kommunens beredskapsplan knyttet til informasjonssikkerhet og personvern.

Risikovurderinger

Alle systemeierne vi intervjuet fortalte at det gjennomføres risikovurderinger (ROS-analyser) og DPIA (ved behov) før et system tas i bruk, og at det er blitt utarbeidet nye ROS-analyser ved store endringer i systemene. Systemeier for Oppvekst fortalte at det også gjennomføres ROS-analyser for applikasjoner før eventuell bruk, og viste til bruk av applikasjonen Youtube på elevenes nettbrett som eksempel. ROS-analysen for Youtube resulterte i at barneskoleelever kun får bruke applikasjonen i kortere perioder på spesifikke datoer, mens på ungdomsskolen er applikasjonen tillatt på elevenes nettbrett etter at elevene har fått undervisning om personvern og bruk av internett. Alle systemeierne bekreftet at de følger kommunens prosedyrer for risikovurderinger som er tilgjengelig i EQS. Systemeier for Helse og mestring fortalte at internkontroll på informasjonssikkerhetsområdet ikke var like godt systematisert som på andre områder, men siden det finnes mange rutiner og prosedyrer i EQS kan man orientere seg ved behov. Revisjonen har fått oversendt dokumentasjon på gjennomførte risikovurderinger i perioden 2021-2025 både gjennom dokumentbestillingen til kommunen og i forbindelse med intervjuer.

[17] Stange kommune (2023). *Kommuneplan 2023-2025 - Samfunnsdel*
[18] Stange kommune (2023). *Helhetlig ROS-analyse 2023-2027*
[19] Beskrivelser av hva som skal gjøres og i hvilken rekkefølge ved uønskede hendelser og kriser.

Tilgangsstyring

Samtlige systemeiere som er intervjuet, fortalte at alle systemer har tilgangsstyring og at tilganger gis eller lukkes som en del av kommunens rutiner for tiltredelse og fratredelse av et arbeidsforhold. Tilganger kan bestilles via Indigo IKT sin tilgangsportal og er knyttet til hvilken rolle som tildeles den ansatte. Ansatte som har fått delegert myndighet av systemeier, eksempelvis nærmeste leder eller systemansvarlig, kan bestille tilganger via tilgangsportalen. Med hensyn til å foreta jevnlige gjennomganger av tilgangene varierer dette i de ulike virksomhetene i kommunen. Systemeier for Oppvekst fortalte at tilgangene i systemene som brukes i barnehage og skole gjennomgås en til to ganger i året i forbindelse med registrering av nye barn og elever, men hadde ikke noe svar på hvor ofte tilgangene i de andre systemene blir gjennomgått eller hvorvidt det er noen rutine eller prosedyre knyttet til dette. Systemansvarlig for arkivtjenesten fortalte at tilgangene gjennomgås ved endringer i virksomhetene, for eksempel ved organisasjonsendringer eller om ansatte endrer stilling. Systemansvarlig for Helse og mestring fortalte at det ikke er noen fast rutine for gjennomgang av tilganger, men at de hadde en større gjennomgang av tilgangene i det ene fagsystemet i løpet av 2024.

Loggføring

Alle systemeiere og systemansvarlige bekreftet at alle systemene har loggføring, og at alle handlinger loggføres. Deriblant åpning og lesing av dokumenter, hvor lenge man har vært inne i deler av systemet, og alle eventuelle endringer. På spørsmål om det er en praksis for jevnlig gjennomgang av logger i Oppvekst eller Helse og mestring, fortalte samtlige intervjuede at gjennomgang av logger er hendelsesbasert og at det har forekommet at kommunen har innhentet logger på forespørsel fra foresatte eller pårørende. Når det gjelder arkivtjenesten fortalte systemansvarlig at logger i praksis gjennomgås daglig ettersom arbeidet til arkivtjenesten krever at de har oversikt over hva som har skjedd i dokumentasjonen og hvilke ansatte som har gjort hva, men at det også har skjedd (svært sjeldent) at logger er blitt gjennomgått for å undersøke snoking.

3.3.2 Årlig gjennomgang av internkontroll

Ifølge kommunens prosedyre *Informasjonssikkerhet – ledelsens gjennomgang* (Stange kommune 2023) gjennomfører kommunedirektørens utvidede ledergruppe, [20] personvernombudet, fagansvarlig, og sikkerhetsansvarlig hos Indigo IKT årlig en gjennomgang av informasjonssikkerheten for å vurdere status på kommunens sikkerhetsarbeid. [21] Fagansvarlig har ansvaret for gjennomføringen av gjennomgangen. Ifølge prosedyren omhandler gjennomgangen temaer som blant annet siste års forebyggende sikkerhetsarbeid, opplæringsbehovet, akseptkriterier for risiko, samt at det besluttes om det skal iverksettes særskilte tiltak knyttet til forebyggende sikkerhet, inkludert sikkerhetsstyringssystemet.

Det blir utarbeidet referat fra ledelsen gjennomgang av kommunens informasjonssikkerhetsarbeid, som lagres i kommunens sak- og arkivsystem unntatt offentlighet. Revisjonen har fått oversendt referat og powerpoint-presentasjon fra det siste møtet 18. februar 2025. Av disse dokumentene fremkommer det at fagansvarlig, sikkerhetsansvarlig i Indigo IKT, samt personvernombudet hadde fått avsatt tid til å snakke om temaene listet opp i prosedyren, før det var en dialog i felleskap og en oppsummering og beslutning om fremtidige tiltak. [22]

[20] Kommunedirektøren, samt alle kommunalsjefer og stabsledere.
[21] Stange kommune (2023). *Informasjonssikkerhet – ledelsens gjennomgang*
[22] Stange kommune (2025). *Powerpoint-presentasjon og møtereferat fra ledelsens gjennomgang for informasjonssikkerhet 18. februar 2025.*

Kommunedirektøren bekreftet i intervju at ledelsens gjennomgang og systemrevisjon av informasjonssikkerheten alltid gjennomføres en gang i året, selv om det kan variere om den gjennomføres på våren eller høsten. Videre forklarte hun at de hele tiden er opptatt av å tenke på hvordan tiltakene som er gjennomført har fungert, og å vurdere hvilke tiltak som videreføres eller eventuelle nye tiltak som må settes inn. Kommunedirektøren opplever at de får belyst tematikk knyttet til informasjonssikkerhet bedre når Indigo IKT også er med som fast deltaker i disse møtene. I møtene diskuteres også blant annet hvilke krav kommunen skal sette til leverandører i anskaffelser av IKT-tjenester, og de har stort fokus på robusthet i løsningene med tanke på kommunens beredskap, fortalte kommunedirektøren.

3.3.3 Opplæringstiltak

Med sikkerhetskultur mener vi at kommunen har overordnede føringer som ligger til grunn for en god praksis innen digital sikkerhet. Herunder handler det om hvordan kommunen sørger for nødvendig kompetanse og sikkerhetsbevissthet blant sine ansatte gjennom relevante opplæringstiltak. Under følger beskrivelser av kommunens rutiner og tiltak for opplæring i informasjonssikkerhet og personvern, samt relevante resultater fra spørreundersøkelsen for å gi et situasjonsbilde av sikkerhetskulturen i kommunen.

Stange kommune har en egen prosedyre som omhandler opplæring i informasjonssikkerhet og personvern. [23] Det er som vist i oversikten kap. 3.3.1 avdelingsledere (ledere med personalansvar) som har ansvar for å sikre at alle ansatte har tilstrekkelig kompetanse og at opplæring i informasjonssikkerhet og personvern blir gjennomført. [24] Fagansvarlig har blant annet i oppgave å bistå med opplæring innen IKT-sikkerhet. Ansatte på sin side har ansvar for å gjøre seg kjent med og følge med på lover, regler, og rutiner, overholde kommunens datavettregler, samt å tilegne seg nødvendig kunnskap for å bruke systemene. Dette inkluderer å gjennomføre sikkerhetsopplæring ved tiltredelse av stilling, samt oppdatering ved behov. [25]

Kommunens datavettregler inneholder generelle regler om passordpraksis, bruk av programvare og saksbehandling knyttet til personopplysninger. [26] Utover dette inneholder dokumentet også informasjon om bruk av teknisk utstyr og programvare, og behandling av sensitive opplysninger. I tillegg definerer datavettreglene hva som skal meldes som avvik og hvordan man gjør dette, samt at det beskrives hvordan den ansatte skal handle ved dataangrep eller når sensitive personopplysninger er på avveie.

Som en del av den generelle opplæringen skal nyansatte gjennomgå kommunens opplæringsskriv om informasjonssikkerhet og personvern og kommunens datavettregler. Ansatte må signere for at de har gjennomgått disse to dokumentene, og revisjonen har mottatt dokumentasjon som viser at dette er gjort. [27] I tillegg må alle ansatte underskrive en databrukeravtale og en taushetserklæring ved ansettelse. Databrukeravtalen lister opp den ansattes forpliktelser og ansvar, samt at det er en bekreftelse på at den ansatte skal følge kommunens rutiner for informasjonssikkerhet. [28] Taushetserklæringen lister opp den ansattes forpliktelser knyttet til å forhindre at uvedkommende får

[23] Stange kommune (2025). *Informasjonssikkerhet og personvern - Opplæringsskriv*
[24] Stange kommune (2023). *Roller, oppgaver og myndighet knyttet til personopplysningsloven*
[25] Stange kommune (2025). *Informasjonssikkerhet og personvern - Opplæringsskriv*
[26] Stange kommune (2025). *Datavettregler*
[27] Stange kommune (2025). *Dokument hentet fra kommunens kvalitetssystem med signaturer fra ansatte*
[28] Stange kommune (2022). *Databrukeravtale*

adgang til sensitiv informasjon som kommunen behandler, og at taushetsplikten også gjelder etter at arbeidsforholdet er avsluttet. [29]

Stange kommune har utarbeidet en liste med definisjoner av sentrale begreper på informasjonssikkerhets- og personvernområdet. [30] Listen ligger i EQS.

Listen inkluderer også en hyperlenke til den delen av personopplysningsloven som gir definisjoner av begrepene brukt i personvernlovgivningen.

Utover opplæringen om informasjonssikkerhet og personvern som er felles for alle ansatte i kommunen, har kommunen også spesifikke opplæringsprosedyrer knyttet til bruk av systemene innen Helse og mestring og arkivtjenesten. Innen Helse og mestring finnes det egne prosedyrer for innføring i bruk av Gerica (elektronisk pasientjournal-system) som en del av introduksjonsrutinene for nyansatte. [31] Dette inkluderer en oversikt over opplæringstiltakene de ulike typene stillinger innen Helse og mestring skal gjennom og tilhørende skriftlige veiledere i fagsystemet. [32] Etter gjennomføring blir prosedyren signert av avdelingsleder og den ansatte før dokumentet legges i den ansattes personalmappe. [33] Når det gjelder ESA (sak- og arkivsystem) har systemansvarlig for arkivtjenesten tidligere arrangert kurs for ansatte som bruker ESA i andre virksomheter i kommunen, samt utarbeidet opplæringsvideoer i bruk av systemet som er lagt ut på kommunens intranett. Samtidig følger arkivtjenesten med på brukerne av ESA, og gir tilbakemeldinger og veiledning dersom de ser ansatte som gjør gjentagende feil.

Kommunen har også benyttet seg av opplæringsmateriale fra eksterne leverandører, nærmere bestemt NanoLæring-kurs fra Junglemap og ulike opplæringstiltak fra Indigo IKT.

NanoLæring består av korte leksjoner (3 minutter) om spesifikke temaer knyttet til informasjonssikkerhet og personvern. Fagansvarlig forklarte at leksjonene er sendt ut månedlig til alle ansatte og blant annet har omhandlet sikkerhetskultur. Kommunen har mulighet til å innhente statistikk som viser gjennomføringsgraden knyttet til NanoLæring-kursene, og revisjonen har fått oversendt denne statistikken for 2023 og 2024. Statistikken viser at 69 % av de ansatte ikke fullførte noen av leksjonen i verken 2023 eller 2024, mens andelen ansatte som fullførte noen av leksjonene var 24 % i 2023 og 18 % i 2024. Andelen ansatte som fullførte alle leksjonene var 7 % i 2023 og 13 % i 2024. [34]

På Indigo IKT sine nettsider finnes det informasjon om digital sikkerhet som er tilgjengelig for alle. Her kan ansatte få informasjon om blant annet generelle sikkerhetsregler og om god passord-praksis.[35]

I 2024 fikk Indigo IKT i oppdrag å formidle KS sin sikkerhetskampanje til ansatte i alle sine eierkommuner. Revisjonen har blitt forelagt statistikk som viser antall klikk på lenkene i sikkerhetskampanjen fra Stange kommune. Statistikken viser at antallet klikk på lenkene synker gradvis

[29] Stange kommune (2022). *Taushetserklæring*
[30] Stange kommune (2023). *Personopplysningsloven - definisjoner*
[31] Stange kommune (2025). *Introduksjonsplan nyansatte helse- og omsorgssenter - sjekkliste*
[32] I ansattportalen finnes det ulike opplæringsskriv for ledere og vanlig ansatte.
[33] Stange kommune (2023). *Sjekkliste for opplæring i GERICA på eget arbeidssted*
[34] Stange kommune (2025). *Powerpoint-presentasjon – Ledelsens gjennomgang*
[35] Indigo IKT.no - Sikkerhet

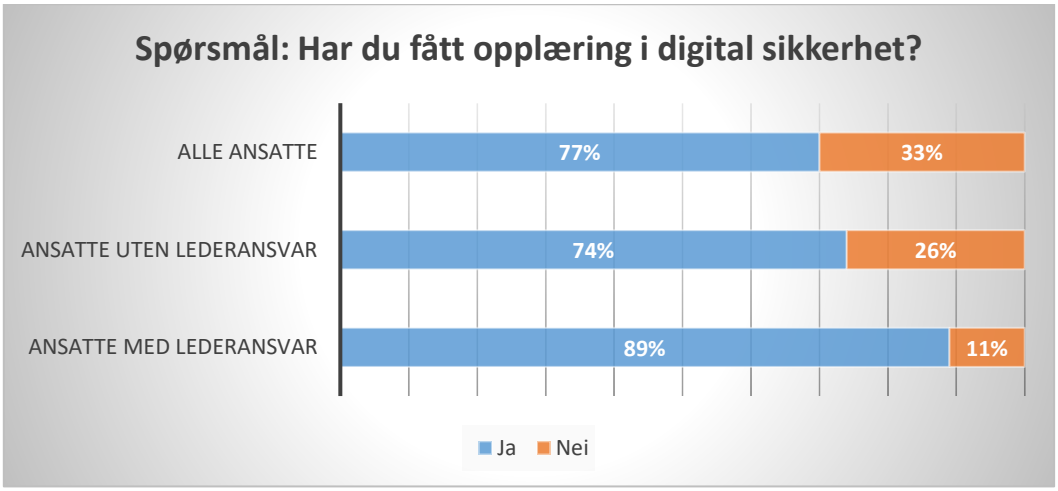
dess lenger ned på listen man kommer, fra 961 klikk på den øverste lenken til 347 klikk på den nederste lenken: [36]

KS Sikkerhetskampanje	Antall klikk på lenke
Tema 1: Låse enheter	961
Tema 2: Passord	711
Tema 3: Pålogging via linker	525
Tema 4: Mobile enheter er personlig	481
Tema 5: Ikke sende sensitive opplysninger på e-post	480
Tema 6: Lagring av informasjon	434
Tema 7: Sikkerhet på hjemmekontor	347

Fagansvarlig fortalte at det kan være utfordrende å nå ut til alle ansatte med hensyn til opplæring i informasjonssikkerhet og personvern, men at opplæringsopplegget har blitt formidlet til alle ledere som har ansvar for å spre og støtte opp om dette i sine egne enheter for å øke gjennomføringen. Videre forklarte fagansvarlig datavettreglene som er utarbeidet er enkle å forstå, og at disse er sendt ut til alle virksomhetsledere slik at de kan spre disse innenfor sine respektive ansvarsområder i tillegg til at reglene finnes lett tilgjengelig i EQS. I EQS har de også mulighet til å sette på en «implementeringsstøtte»-funksjon slik at de kan hente ut informasjon om hvilke ansatte som har åpnet spesifikke dokumenter. Denne funksjonen er ikke aktivert på alle dokumenter i EQS, men fungerer bra dersom man aktiverer den avdelingsvis for å undersøke om ansatte har lest dokumenter. Fagansvarlig fortalte også at hun har planlagt å utarbeide en egen opplæringsplan spesifikt om informasjonssikkerhet.

Spørreundersøkelsesdata

I spørreundersøkelsen ble respondentene spurt om de hadde fått opplæring i digital sikkerhet. I diagrammet under fremkommer det hva respondentene svarte:



Kilde: Revisjon Øst/Questback N=537/432/103

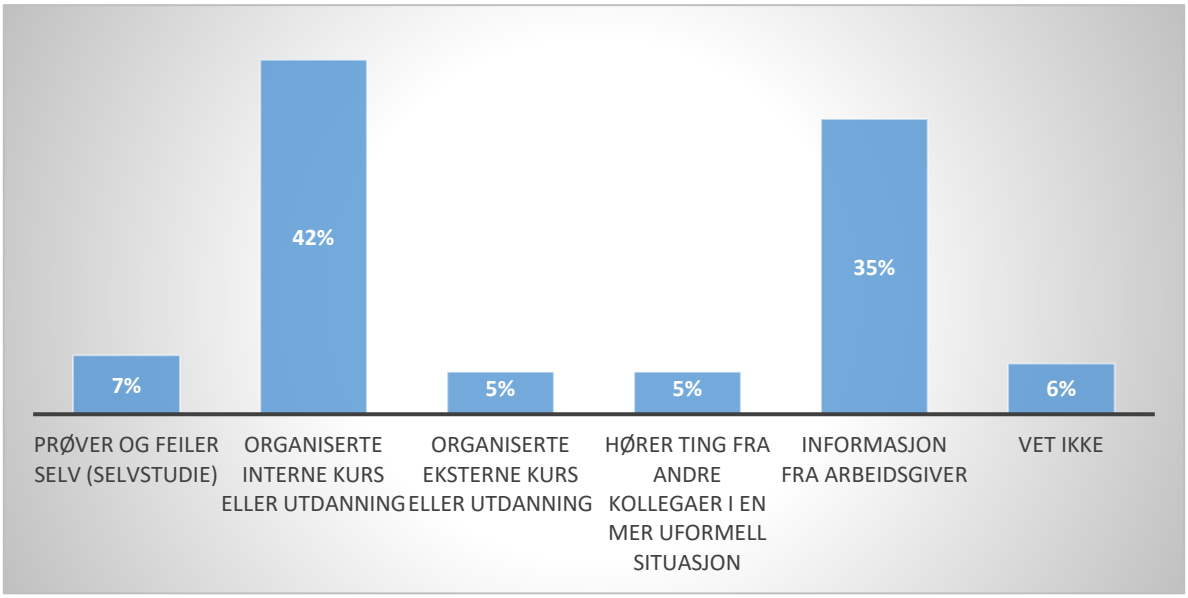
Svarene viser at 77 % av alle respondentene har fått opplæring i digital sikkerhet. For respondentene uten eller med lederansvar svarer henholdsvis 74 % og 89 % at de har fått slik opplæring.

[36] Stange kommune (2025). *Powerpoint-presentasjon – Ledelsens gjennomgang*

Med hensyn til den enkelte avdeling var det kun i fire avdelinger at mindre enn 75 % av de ansatte svarte at de hadde fått opplæring i digital sikkerhet. De fire avdelingene som skilte seg ut med en noe lavere svarprosent var:

- Tilrettelagte tjenester (53 % av 49 respondenter) [37]
- Barnehage (60 % av 35 respondenter) [38]
- Ungdomsskole (71 % av 48 respondenter)
- Helsetjenester i hjemmet (74 % av 19 respondenter)

Videre i spørreundersøkelsen ble respondentene spurt hvordan de vanligvis lærer om digital sikkerhet, og de ble gitt flere alternativer. Diagrammet under viser hva respondentene svarte:



Kilde: Revisjon Øst/Questback N=535

Svarene viser at 77 % av respondentene vanligvis får opplæring i digital sikkerhet gjennom opplæringstiltak eller informasjon fra arbeidsgiver. På spørsmål om hvilke temaer de ansatte ønsker mer kunnskap om var det flest som svarte digitale trusler (60 %), sky-tjenester (47 %), og varsling av sikkerhetshendelser i egen virksomhet (41 %).

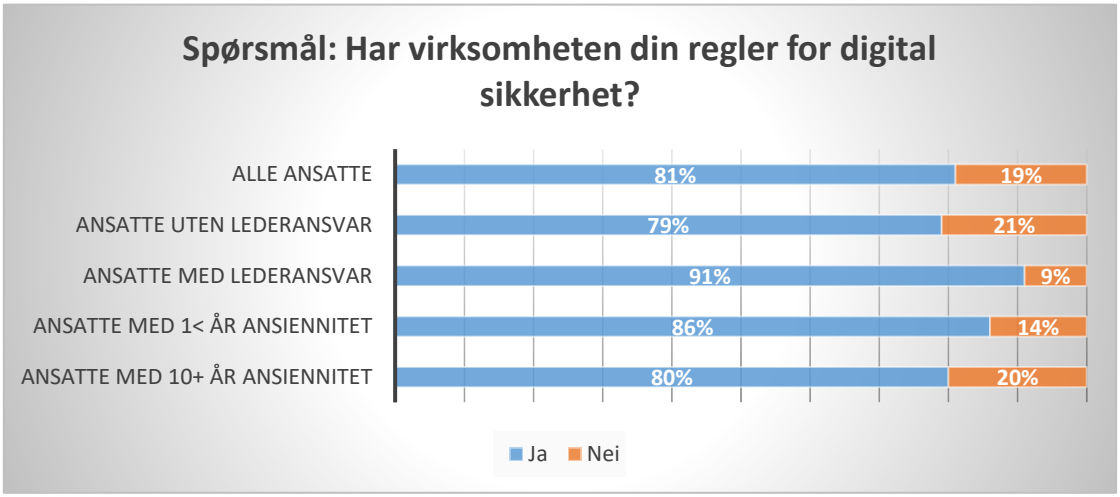
Spørreundersøkelsen inkluderte spørsmål som omhandlet i hvilken grad den ansatte er i stand til å vurdere hva som trygt eller utrygt å gjøre på internett. 92 % av 535 respondenter svarte at de i stor grad er i stand til å vurdere dette på egenhånd. På spørsmål om man forbinder bruk av epost med høy risiko, var det 68 % av 529 respondenter som svarte at de i liten grad forbinder dette med høy risiko. Samtidig svarte 18 % av 534 respondenter at de ikke forbinder deling av jobb-passord med andre med høy risiko, og 26 % av 536 respondenter oppga at de ikke forbinder mottak av SMS-er med lenker med høy risiko.

I spørreundersøkelsen ble det også stilt spørsmål knyttet til de ansatte sin sikkerhetsatferd. 4 % av 537 respondenter oppga at de ikke kontrollerer nettsider før de bruker dem og 5 % av 537 respondenter oppga at de ikke kontrollerer lenker og vedlegg mottatt på epost før de åpner dem. Videre svarte 62

[37] Merk at svarprosenten på spørreundersøkelsen i enheten var 14 %.
[38] Merk at svarprosenten på spørreundersøkelsen i enheten var 24 %.

% av 537 respondenter at de ikke bruker samme passord i flere av systemene de bruker i jobbsammenheng, og 90 % av 538 respondenter svarte at de ikke bruker samme passord hjemme som på jobb. På spørsmål om man låser skjermen når man forlater datamaskinen, svarte 82 % av 537 respondenter at de alltid eller som regel gjør det, mens 11 % svarte at de gjør det av og til, og 7 % svarte at de ikke gjør det.

I spørreundersøkelsen ble respondentene også spurt om de var kjent med virksomhetens regler for digital sikkerhet, enten egne for avdelingen eller regler som gjelder for hele kommunen. I diagrammet under fremkommer det hva respondentene svarte:



Kilde: Revisjon Øst/Questback N=538/432/104/210/50

Svarene viser at 81 % av respondentene er kjent med virksomhetens regler for digital sikkerhet. For respondentene uten eller med lederansvar svarer henholdsvis 79 % og 91 % at de er kjent med disse. Svarene viser at det også er forskjeller blant ansatte med ulik ansiennitet. 86 % av respondentene med under 1 års ansiennitet er kjent med virksomhetens regler for digital sikkerhet, mens 80 % av respondentene med over 10 års ansiennitet svarer det samme.

Kommunedirektøren forklarte at de har egne opplæringsskriv knyttet til informasjonssikkerhet i EQS, samt et eget dokument med begrepsforklaringer ettersom det er viktig å definere de ulike begrepene på informasjonssikkerhetsområdet. Kommunedirektøren erkjenner at kommunen har et forbedringspotensial med hensyn til å spisse opplæringen med tanke på de ansattes egen rolleforståelse, og at noe av det mest utfordrende er å oversette opplæringsopplegget knyttet til informasjonssikkerhet slik at alle ansatte kan forstå det. Samtidig har de sett en forbedring innenfor deler av sikkerhetskulturen i kommunen ettersom det er færre og færre ansatte som biter på svindelforsøk. Sist gang det ble sendt suspekte eposter til ledere i kommunen var det ingen som ble lurt, fortalte kommunedirektøren.

3.4 Innhentet data: Avvik (kriterie 7-8)

3.4.1 Avviksregistrering

Ansatte i Stange kommune har ifølge prosedyren *Roller, oppgaver og myndighet knyttet til personopplysningsloven* (Stange kommune 2023) et selvstendig ansvar for å melde avvik og uønskede hendelser knyttet til informasjonssikkerhet, samt å gjøre seg kjent med kommunens rutiner for å melde avvik. Alle avvik skal meldes gjennom et standardisert skjema i EQS i henhold til kommunens

prosedyre for avviksregistrering. [39] Virksomhetsledere har ansvar for at avviksprosedyren er kjent for de ansatte og tilrettelegging for gjennomføring av avviksregistrering. Avdelingsledere har ansvar for å gjennomføre den praktiske tilretteleggingen i egen tjeneste og sørge for løpende behandling av avviksmeldinger. Avviksprosedyren inneholder fire ulike definisjoner som de ansatte skal bruke til å avgjøre hvordan et avvik skal kategoriseres og meldes. Det som defineres er hvorvidt hendelsen er meldepliktig, om hendelsen utgjør et avvik som bryter med lovverk og føringer, om hendelsen er uønsket og om hendelsen er meldeverdig med hensyn til omfang.

I avviksregistreringsskjemaet fyller den ansatte inn i hvilken enhet avviket skjedde og hvilken enhet som skal behandle avviket, samt hvilken kategori avviket tilhører basert på definisjonene nevnt over. Den ansatte velger ut ifra dette hvilket skjema som skal fylles ut. Avviksregistreringssystemet har en innebygd funksjon som gjør at skjemaet endrer seg dersom man huker av for spesifikke faktorer. Eksempelvis vil skjemaet endre seg automatisk til et skademeldingsskjema dersom man huker av for at hendelsen førte til personskade. I prosedyren er det også beskrevet at avviksmeldinger ikke skal inneholde sensitive opplysninger. Den ansatte kan når som helst logge inn i kvalitetssystemet og se status på sine egne innmeldte avviksmeldinger.

Stange kommune har også ifølge ovenfor nevnte prosedyre en forventning til eksterne databehandlere de har avtaler med, om at de melder inn eventuelle avvik til kommunens fagansvarlig.

Alle systemeiere og systemansvarlige vi intervjuet bekreftet at alle avvik skal meldes i EQS. Revisjonen fikk videre opplysninger om at det generelt meldes få avvik knyttet til informasjonssikkerhet og personvern, men i de tilfellene hvor det har forekommet har disse blitt meldt i EQS. Systemeier for arkivtjenesten fortalte at det er hver enkelt leder sitt ansvar å ta opp med sine ansatte hva som utgjør et avvik, samt å ufarliggjøre det å melde avvik. Selv har han brukt mye tid på dette med sine egne ansatte. Videre fortalte systemeieren for arkivtjenesten at det er en utfordring for enkelte ansattgrupper å melde avvik i EQS. Dette gjelder ansattgrupper som ikke vanligvis sitter foran en datamaskin, og at det da kan oppleves som tungvint å reise til virksomhetens kontorsted for å logge seg inn i EQS og melde avvik. På grunn av dette har de arbeidet med å gi disse ansattgruppene tilgang til EQS via mobilen.

Systemeier for Helse og mestring fortalte at det i EQS gis en advarsel til de ansatte om at avviksmeldinger ikke skal inneholder sensitive personopplysninger, og at de ansatte er flinke til å overholde dette.

Kommunens databehandlere skal ifølge kommunens prosedyrer rapportere om sikkerhetsavvik dersom dette blir oppdaget. Systemeier for Oppvekst bekreftet at leverandører av systemer selv har tatt kontakt med kommunen dersom de oppdager feil i sine systemer, og at kommunen har fått god informasjon om hvordan avviket påvirker Stange kommune spesifikt.

I spørreundersøkelsen ble det stilt spørsmål om den ansatte er klar over hvem det skal meldes fra til om digitale sikkerhetshendelser. For dette spørsmålet ble de som svarte bekreftende ledet til et oppfølgingsspørsmål, hvor de ble bedt om å skrive i et åpent tekstfelt hvem de skal melde fra til. Det var 439 personer (82 %) som svarte at de vet hvem de skal melde fra til om digitale sikkerhetshendelser, og 381 personer (71 %) som svarte på oppfølgingsspørsmålet. Av svarene på oppfølgingsspørsmålet oppga de aller fleste at de skal melde fra til nærmeste leder og Indigo IKT, samt

[39] Stange kommune (2025). *Melding av hendelser, avvik og skademelding - prosedyre*

fagansvarlig i Stange kommune. Enkelte svarte også at de ville rapportere hendelsen til Datatilsynet eller registrere den i kommunens avvikssystem.

3.4.2 Oppfølging av avvik

Ifølge kommunens prosedyrer skal systemeiere ved avvik knyttet til informasjonssikkerhet eller personvern, orientere fagansvarlig. [40] Avviket skal deretter håndteres av fagansvarlig og sikkerhetsansvarlig hos Indigo IKT, i samråd med relevant systemeier og avdelingsleder, samt eventuelt relevant databehandler. Kommunedirektøren forklarte i intervju at de har en praksis for å håndtere og lukke avvik på lavest mulig nivå i kommunen, og at ledere er flinke til å vurdere hva som burde meldes videre til kommunedirektøren. Dersom avviket har medført brudd på personopplysningssikkerheten og det skal meldes avvik til Datatilsynet skal personvernombudet kobles på.

Videre i kommunens prosedyrer er det beskrevet at behandlingen av avviket skal være påbegynt senest 14 dager etter at avviksmeldingen er sendt, men om det er et alvorlig avvik skal det behandles uten ugrunnet opphold. [41] I den innledende behandlingen skal meldingsansvarlig kontakte vedkommende som har meldt avviket dersom det er behov for nærmere avklaringer, samt vurdere om eventuelle strakstiltak er tilstrekkelig. Saken skal ikke lukkes i EQS før man er sikker på at avviket faktisk er håndtert. Ved iverksettelse av tiltak skal disse alltid beskrives og det skal utpekes en person som er ansvarlig for å gjennomføre tiltaket, i tillegg til at det registreres en tidsfrist for oppfyllelse. Dersom oppfølgingen krever samarbeid på tvers av virksomheter finnes det funksjoner i EQS for å gi andre mulighet til å lese eller overta saksgangen. Når tiltak er gjennomført skal tiltaksansvarlig rapportere dette i EQS, og meldingsansvarlig godkjenner tiltakene og lukker saken. Ved lukking av saken skal meldingsansvarlig fylle ut en kort evaluering av effekten av tiltak og prosessene som er gjennomført, samt skrive en kommentar om årsaken til at avviket lukkes.

Systemeierne og de systemansvarlig vi intervjuet fortalte kommunens prosedyre for avviksoppfølging også gjaldt avvik knyttet til informasjonssikkerhet og personvern, men gjentok at det har vært få avvik av denne typen. Ved slike avvik er det vanlig at fagansvarlig, Indigo IKT, personvernombudet, og eventuelt eksterne databehandlere også er involvert i oppfølgingen, fortalte flere. Systemeierne for Oppvekst og arkivtjenesten forklarte at de har ansvar for å dokumentere oppfølgingen og lukke avviket i EQS, men at de ikke håndterer oppfølgingen alene og vurderer hvem som må kobles på avhengig av typen avvik. Eksempelvis blir fagansvarlig og personvernombudet koblet på dersom avviket omhandler personvern. Systemeier for Oppvekst forklarte at avvik knyttet til informasjonssikkerhet og personvern blir håndtert og lukket raskt.

Revisjonen bad systemeierne og de systemansvarlige om å fortelle om avvik knyttet til informasjonssikkerhet og personvern innenfor sitt virksomhetsområde i perioden 2020-2025. Totalt var det snakk om syv avvik, fire innen Oppvekst og tre innen arkivtjenesten. Av eksemplene fremkom det at fagansvarlig, personvernombudet, og Indigo IKT har blitt involvert i sakene som var knyttet til kommunens datasystemer og/eller personvern. Videre fortalte systemeierne og de systemansvarlige at avvikene ble håndtert i henhold til kommunens prosedyrer, inkludert at oppfølgingen ble dokumentert i EQS. I tillegg viste begge systemeierne til at enkelte av avvikene hadde ført til læring og endring i rutiner i etterkant av hendelsene. Innen Helse og mestring hadde det ikke forekommet noen

[40] Stange kommune (2023). *Roller, oppgaver og myndighet knyttet til personopplysningsloven*
[41] Stange kommune (2025). *Behandling av melding – avvik og hendelser*

slike avvik i perioden, men de hadde hatt enkelte mindre uønskede hendelser som skyldtes software-problemer i et fagsystem hvor feilene var blitt rettet så snart de ble oppdaget av systemansvarlig.

Fagansvarlig fortalte i intervju at hun er involvert i oppfølgingen av avvik på informasjonssikkerhetsområdet, og at enkelte slike avvik følges opp i samarbeid med andre kommuner ettersom det er en del interkommunalt samarbeid knyttet til informasjonssikkerhet. Dersom avviket omhandler personvern, blir personvernombudet også involvert. Om avviket må meldes til Datatilsynet er det fagansvarlig melder ifra, mens personvernombudet bidrar med vurderinger.

Revisjonen bad kommunedirektøren om å fortelle om oppfølgingen av avvik på informasjonssikkerhetsområdet i perioden 2020-2025. Kommunedirektøren fortalte først om et stort datainnbrudd hos Indigo IKT (selskapet het på daværende tidspunkt Hedmark IKT (HIKT)). Daglig leder i HIKT tok kontakt med Stange kommune og kommunedirektøren med sin ledergruppe ble varslet. I håndteringen av hendelsen ble selskapets beredskapsplan fulgt, og det var en struktur med jevnlige tilbakemeldinger fra daglig leder i selskapet til kommunen, og kommunedirektøren ble betrygget av måten selskapet arbeidet på. I etterkant av hendelsen ble beredskapsplanen til selskapet oppdatert med utgangspunkt i erfaringer de hadde tatt fra hendelsen. Utover dette har det vært flere mindre hendelser hos Indigo IKT eller avvik knyttet til spesifikke fagsystemer i kommunen. Ved de mindre hendelsene hos Indigo IKT har kommunen blitt informert nå hendelsen er løst, noe kommunedirektøren mente var riktig måte å gjøre det på ettersom hendelsene ikke hadde noen konsekvenser for eierkommunene. Når det gjelder avvik knyttet til spesifikke fagsystemer så har kommunens fagansvarlig raskt blitt koblet på og fulgt opp avvikene.

3.5 Revisors vurdering

3.5.1 Vurdering av revisjonskriterium 1 – Sikkerhetsmål og sikkerhetsstrategi

Undersøkelsen viser at Stange kommune har et overordnet sikkerhetsmål knyttet til personvernprinsippene, samt en sikkerhetsstrategi basert på operasjonelle tiltak som spesifikt beskriver hvordan kommunen skal ivareta hvert av prinsippene i informasjonssikkerhetsarbeidet.

I kommunens kvalitetssystem EQS? lagres dokumenter som omhandler informasjonssikkerhet og personvern fargekodet og oversiktlig organisert slik at ansatte enkelt kan finne frem til styrende (grønne), gjennomførende (gule, og kontrollerende) dokumenter. I tillegg er kommunens sikkerhetsmål og personvernprinsippene som danner grunnlaget for sikkerhetsstrategien beskrevet i det obligatoriske opplæringsskrivet om informasjonssikkerhet som alle nye ansatte skal gjennomgå.

Vi mener derfor at kommunen ivaretar krav til sikkerhetsmål innen informasjonssikkerhet og personvern, samt at kommunen har en oversiktlig strategi for å nå disse målene. Vi vurderer også at kommunen i tilfredsstillende grad tilrettelegger for at mål og strategier er kjent for de ansatte.

Vi mener at revisjonskriterium 1 er etterlevd.

Kommunen må ha utarbeidet sikkerhetsmål og en sikkerhetsstrategi, og strategien må være kjent for de ansatte.

3.5.2 Vurdering av revisjonskriterium 2 – Sikkerhetsorganisasjon

Undersøkelsen viser at Stange kommune har en oversikt over kommunens sikkerhetsorganisasjon som viser de spesifikke ansvarsoppgavene til alle de ulike aktørene i informasjonssikkerhetsarbeidet, fra kommunedirektøren på toppen ned til de ansatte som brukere av systemene.

I tillegg inkluderer oversikten hvilke forventninger kommunen har til Indigo IKT og eksterne leverandører, med beskrivelser av spesifikke oppgaver i informasjonssikkerhetsarbeidet som kommunen forventer at de bidrar til eller ivaretar.

Vi mener at revisjonskriterium 2 er etterlevd.

Kommunen må ha en sikkerhetsorganisasjon med beskrivelser av ansvar og roller for informasjonssikkerhet.

3.5.3 Vurdering av revisjonskriterium 3 – Oversikt over sentrale informasjonsverdier

Våre undersøkelser viser at beredskapsplanen til Indigo IKT inkluderer en oversikt over kommunens viktige informasjonsverdier med tilhørende kritikalitetsvurderinger, samt at det pågår et arbeid for å utarbeide en policy for klassifisering av informasjon. En slik oversikt er en viktig del av risikostyringen og er et godt grunnlag for beredskapsplanlegging og hendelseshåndtering, da det gir kommunen mulighet til å prioritere hvilke ressurser som trenger mest beskyttelse ved et dataangrep eller lignende.

Vi mener at revisjonskriterium 3 er etterlevd.

Kommunen må ha skaffet oversikt over sentrale informasjonsverdier og hvor kritiske disse er for kommunens drift og tjenesteproduksjon.

3.5.4 Vurdering av revisjonskriterium 4 – Internkontroll

Stange kommune har et internkontrollsystem for informasjonssikkerhet og personvern som inkluderer internkontrollaktivitetene beskrevet i KS sin veileder for personvern og informasjonssikkerhet. Dette omfatter også kontrolleraktiviteter og roller som sørger for at internkontrollsystemet fungerer som forutsatt og bidrar til videreutvikling av internkontrollen.

Oversikten over de ulike aktørene i informasjonssikkerhetsarbeidet og deres ansvarsoppgaver bidrar til å sikre at alle ansatte vet hvilke funksjoner de skal ivareta i internkontrollarbeidet, samt sørger for at eksterne leverandører også er delaktig i internkontrollen.

På bakgrunn av innhentet data vurderer revisjonen at aktørene i informasjonssikkerhetsarbeidet i tilfredsstillende grad ivaretar sine funksjoner i internkontrollen i henhold til kommunens prosedyrer, samt sørger for at informasjonssikkerhet og personvern er et tema i kommunens beredskapsarbeid og øvelser.

Vi mener at revisjonskriterium 4 er etterlevd.

Kommunen må ha en internkontroll som omfatter informasjonssikkerhet og personvern, herunder etablere aktiviteter som sikrer at internkontrollen gjennomføres og fungerer som forutsatt.

3.5.5 Vurdering av revisjonskriterium 5 – Årlig gjennomgang av internkontroll

Kommunens prosedyre for ledelsens gjennomgang og systemrevisjonen av informasjonssikkerhet, bidrar til å sikre at internkontrollsystemet for informasjonssikkerhet og personvern gjennomgås minst en gang i året. Den sørger også for å forankre informasjonssikkerhetstiltak ved at hele kommunens organisasjon er representert i gjennomgangen.

Revisjonen mener det er bra at Indigo IKT sin deltakelse er forankret i den nevnte prosedyren, og at kommunen dermed kan dra veksler på Indigo sin kompetanse i gjennomgangen av informasjonssikkerheten. Vi vurderer at kommunen på denne måten i større grad sørger for å ha en helhetlig oversikt over risikosituasjonen. Totalt sett gjør dette at kommunen etter vår vurdering i tilfredsstillende grad er i stand til å sette inn treffsikre forebyggende informasjonssikkerhetstiltak.

Vi mener at revisjonskriterium 5 er etterlevd.

Systemet for internkontroll innen informasjonssikkerhet og personvern bør gjennomgås årlig.

3.5.6 Vurdering av revisjonskriterium 6 – Opplæringstiltak

Undersøkelser viser at kommunen har rutiner for generell opplæring i informasjonssikkerhet og personvern felles for alle nye ansatte, inkludert en liste med definisjoner av sentrale begreper som kan brukes som et oppslagsverk av de ansatte. Kommunen har også egne opplæringsrutiner knyttet til bruk av spesifikke fagsystemer.

Kommunen har en utfordring med å få alle ansatte til å ta i bruk opplæringsmateriale om informasjonssikkerhet, og spørreundersøkelsen viser at en fjerdedel av de ansatte oppgir at de ikke har fått opplæring i digital sikkerhet. Resultatene fra spørreundersøkelsen viser at en stor andel ansatte selv mener de kan vurdere hvilke digitale aktiviteter som innebærer høy risiko. Over halvparten av de som har svart på spørsmålet mener det er liten risiko knyttet til bruk av e-post, og 18 % oppgir at det ikke er forbundet høy risiko ved deling av passord. Videre oppgir cirka en femtedel av de ansatte at de ikke kjenner til at kommunen har regler for digital sikkerhet. Dette gjelder i størst grad ansatte med lengst ansiennitet. Det er viktig å merke seg at tallene for enkelte av enhetene ikke nødvendigvis er representative. Revisjonen vil her minne om at innholdet i eposter ikke er sikret på noen måte, og ukryptert epost går ikke direkte fra sender til mottaker, men via mange forskjellige knutepunkt før den kommer frem. Samtidig må revisjonen påpeke at deling av passord øker sjansen for at passord havner på avveie, og konsekvensene ved at uvedkommende får tak i ansattes passord og får tilgang til kommunens systemer kan være svært alvorlige. Ifølge Datatilsynet er misbruk av brukernavn og passord ofte den enkleste og raskeste veien inn til virksomhetens nettverk og informasjonssystem, i tillegg er epostangrep som utnytter folks tendens til å bruke samme brukernavn og passord på tvers av kontoer en økende sikkerhetstrussel. Alt i alt indikerer funn i undersøkelsen at kommunen har et forbedringspotensial når det gjelder ulike opplæringstiltak, samt når det gjelder å tydeliggjøre forventninger til at ansatte skal gjøre seg kjent med sentrale dokumenter på området. Revisjonen vurderer at manglende opplæring øker risikoen for digitale sikkerhetsbrudd.

Vi mener derfor at revisjonskriterium 6 er delvis etterlevd.

Kommunen må ha tiltak som sikrer at ansatte får opplæring knyttet til informasjonssikkerhet og personvern.

3.5.7 Vurdering av revisjonskriterium 7 – Avviksregistrering

Undersøkelsen viser at kommunens praksis for avviksregistrering ivaretar en systematikk og er en integrert del av kommunens kvalitetssystem. I tillegg inkluderer avviksprosedyrene definisjoner som gjør det enklere for ansatte å vite hva som skal registreres i systemet, samt å kategorisere hendelsene som meldes inn. Vi mener også det er hensiktsmessig at det finnes en funksjon i avvikssystemet som gir ansatte en automatisk advarsel om at avviksmeldinger ikke skal inneholde sensitive personopplysninger, for å forhindre at slik informasjon blir liggende i kommunens kvalitetssystem.

Med hensyn til avvik på informasjonssikkerhetsområdet, presiserer kommunens rutiner en forventning til eksterne leverandører når det gjelder hvor leverandørene skal melde inn avvik som påvirker kommunen. Dette mener vi er en god praksis.

Intervju med nøkkelpersoner i virksomhetsområdene viser til at kommunens avviksprosedyre følges, og resultater fra spørreundersøkelsen indikerer at de aller fleste vet hvor og hvem de skal melde fra til om digitale sikkerhetshendelser.

Vi mener at revisjonskriterium 7 er etterlevd.

Kommunen må ha et system for avviksregistrering innenfor informasjonssikkerhet og personvern.

3.5.8 Vurdering av revisjonskriterium 8 – Oppfølging av avvik

Undersøkelser viser at det har vært få avvik på informasjonssikkerhet- og personvernområdet i kommunen i perioden 2020-2025, men i de tilfellene hvor det har forekommet, har relevante aktører blitt koblet på. Videre viser undersøkelsen at kommunen har en årlig gjennomgang av internkontrollen på informasjonssikkerhetsområdet, som inkluderer en diskusjon om håndteringen av uønskede hendelser. Dette mener vi er en god praksis som sikrer at kommunen bruker erfaringer fra avvikshåndtering til å forbedre sin praksis på området. Flere vi snakket med kunne vise til konkrete eksempler hvor avvikshåndtering hadde ført til endret praksis på informasjonssikkerhetsområdet.

Vi mener at revisjonskriterium 8 er etterlevd.

Avvik må gjennomgås, håndteres, og brukes for forbedring av prosedyrer og praksis i ivaretakelsen av informasjonssikkerhet og personvern.

4 Problemstilling 2 – Personvern

Har Stange kommune etablerte rutiner og praksis som sikrer et tilfredsstillende vern av fysiske personer i forbindelse med behandling av personopplysninger?

4.1 Revisjonskriterier for problemstilling 2

Nedenfor er en oversikt med de kriterier vi har benyttet for å besvare problemstillingen og våre vurderinger av disse. Kriteriene er gjengitt i kortform. For en full utledning av revisjonskriteriene, se vedlegg A.

	Kriterium 9	Kommunen må ha et personvernombud etter regelverket, og sørge for at personvernombudet er kjent for de ansatte og andre.
	Kriterium 10	Kommunen må ha nødvendige rutiner, prosedyrer, og praksis som sikrer tilfredsstillende håndtering av personopplysninger, og som oppdateres ved behov.
	Kriterium 11	Kommunen må føre protokoller over alle behandlingsaktiviteter.
	Kriterium 12	Kommunen må gi informasjon om hvordan de behandler personopplysninger, gjennom en personvernerklæring.
	Kriterium 13	Kommunen må sørge for at det foreligger databehandleravtaler med og mellom virksomheter som behandler personopplysninger på vegne av kommunen, og disse må være i henhold til personvernlovgivningen.

4.2 Innhentet data: Personvernombud (kriterie 9)

En kjøpsavtale revisjonen har fått oversendt viser til at Stange kommune samarbeider om personvernombudtjenester med Hamar kommune og Løten kommune. [42] I kjøpsavtalen mellom de tre kommunene er det beskrevet at personvernombudets hovedoppgave er å informere og gi råd til behandlingsansvarlige eller databehandlere om de forpliktelsene kommunene har etter personvernlovgivningen. Videre er det beskrevet at personvernombudets hovedsete er Hamar kommune, og at Stange kommune og Løten kommune stiller kontorplass til disposisjon ved behov. Etter avtalen er personvernombudet tilsatt i Hamar kommune med 100 % stilling, hvorav 80 % av stillingen innebærer å ivareta personvernombudsrollen for de tre samarbeidskommunene.[43]

I kommunens oversikt over roller og ansvar knyttet til personopplysningsloven, er det beskrevet at personvernombudet har en uavhengig rolle, og skal bidra til kommunens personvernarbeid gjennom rådgivning, kontroll, og nødvendig bistand for å sikre at kommunen overholder lovverket. Dette innebærer at personvernombudet skal bistå ved gjennomføring av DPIA, være kontaktpunkt mellom kommunen og Datatilsynet, samt å ta imot henvendelser fra de registrerte. [44]

[42] Stange kommune (2019). *Avtale om kjøp av tjeneste som personvernombud mellom Løten, Stange og Hamar kommuner*

[43] Den øvrige ressursen på 20 % skal dekke vertskommunevirksomhetene der Hamar har ansvaret og mange kommuner deltar; 110-sentralen, Hamar interkommunale krisesenter, og Hedmark IKT (HIKT). Hedmark IKT endret navn til Indigo IKT 1. januar 2023.

[44] Stange kommune (2023). *Roller, oppgaver og myndighet knyttet til personopplysningsloven*

Som en del av datainnsamlingen i forbindelse med forvaltningsrevisjonen fikk kommunens personvernombud tilsendt en spørsmålsliste som omhandlet personvernombudstjenestene som blir levert til Stange kommune.

På spørsmål om hvilke oppgaver personvernombudet ivaretar for, eller i samarbeid med kommunen, ble revisjonen informert om at han gir kommunens ledelse, ansatte, og innbyggere råd om plikter og rettigheter etter personvernlovgivningen, og kontrollerer kommunens overholdelse av regelverket. Dette innebærer at personvernombudet blir involvert i spørsmål av betydning for personvernet, særlig relatert til personvernkonsekvensvurderinger (DPIA), avvik, rutiner, databehandleravtaler, anskaffelser, internkontroll, tilsyn og revisjonen. I tillegg holder personvernombudet presentasjoner om ulike personvernrelaterte tema. Personvernombudet vier mye tid og oppmerksomhet til etablering av felles styringssystem for personvern og informasjonssikkerhet i Indigo-samarbeidet.

Med hensyn til kontakten mellom kommunen og personvernombudet forklarte han at fagansvarlig er hans primærkontakt i Stange kommune, og at det i tillegg forekommer at personvernombudet får direkte henvendelser fra ansatte og publikum. Videre følger personvernombudet opp ulike områdespesifikke systemansvarlige, hovedsakelig i forbindelse med møter i deres respektive fagråd (Sektorforum) i Indigo-samarbeidet.

Revisjonen spurte deretter om personvernombudet har fått opplæring knyttet til utøvelsen av vervet. Personvernombudet fortalte at han har fagutdanning innen rettsinformatikk og lang arbeidserfaring med informasjonssikkerhet og personvern, samt deltar i flere kompetansenettverk med fokus på personvernombudsrollen. Dette er Foreningen personvernombudene, Foreningen kommunal informasjonssikkerhet, og Nettverk for informasjonssikkerhet i regi av Digitaliseringsdirektoratet hvor det løpende holdes samlinger og møter om ombudsrelaterte tema.

På spørsmål om personvernombudet bidrar til opplæring av ansatte i personvern, forklarte han at dette skjer i liten grad. Det har skjedd på forespørsel og ved kapasitet, men hovedfokuset til personvernombudet er å veilede den sikkerhetsansvarlige hos Indigo IKT og eierkommunenes fagansvarlige for informasjonssikkerhet og personvern, slik at disse igjen kan sikre opplæring av andre ansatte.

Revisjonen spurte også hvordan Stange kommune ivaretar henvendelser fra innbyggerne rundt personvernspørsmål. Personvernombudet fortalte at innbyggere henvises til kommunens fagansvarlig som henviser videre til personvernombudet om vedkommende ikke kan svare på henvendelsen selv. Kontaktopplysningene til personvernombudet er publisert på kommunens nettside, og det hender at henvendelser fra innbyggerne kommer direkte til personvernombudet.

Personvernombudet ble også stilt spørsmål ved om på hvilke måter han kontrollerer at Stange kommune overholder personvernregelverket. Personvernombudet forklarte at dette blant annet skjer gjennom deltakelse i ledelsens (årlige) gjennomgang og systemrevisjon av informasjonssikkerhet, samt gjennom jevnlig kontakt med fagansvarlig. Personvernombudet la til at kontrollvirksomheten vil få større fokus når et felles styringssystem er etablert, og regner med å gjennomføre kontroll opp mot dette systemet i løpet av høsten 2025.

Revisjonen stilte også spørsmål vedrørende personvernombudets hjelp til kommunen i forbindelse med gjennomføring av DPIA. Personvernombudet fortalte at han bistår kommunen med gjennomføring av DPIA på forespørsel. Dette er gjort blant annet ved anskaffelsen av systemene

Microsoft365, velferdsteknologiplattformen, og KOBO.[45] Bistanden til personvernombudet består som regel av deltakelse i arbeidsmøter hvor løsningen blir vurdert etter mal-verktøyet for DPIA, som personvernombudet har vært med på å utvikle.

Avslutningsvis spurte revisjonen hvordan personvernombudet samarbeider med Datatilsynet. Personvernombudet fortalte at han har løpende kontakt med Datatilsynet gjennom de ulike nettverkene han deltar i, samt at han deltar på arrangementer i regi av Datatilsynet. Det hender at personvernombudet tar kontakt med Datatilsynets veiledningstjeneste eller tilsynets eget personvernombud ved behov for råd om spesifikke spørsmål. I tillegg har personvernombudet kontakt med Datatilsynet i forbindelse med enkeltsaker, avvik og tilsyn. Personvernombudet formidler deretter Datatilsynets råd videre til sine kontakter i Indigo IKT og eierkommunene. Personvernombudet fortalte også at det er blitt gjennomført veiledningsmøter med Datatilsynet for å avklare krevende juridiske spørsmål i forbindelse med IT-utviklingsprosjekter. Mye av dialogen med Datatilsynet omhandler oppbygningen av Samsvar i Indigo-samarbeidet, for å sikre at systemet bygges på en slik måte at det tilfredsstiller kravene til Datatilsynet.

I intervju ble kommunedirektøren spurt om ordningen dekker kommunens behov for personvernombudstjenester. Kommunedirektøren fortalte at hun hadde vært mer tilbakeholden til å svare ja dersom spørsmålet hadde blitt stilt for noen år siden, men at det fungerer bra nå siden personvernombudet er mer involvert i Indigo-samarbeidet. Kommunedirektøren opplever at personvernombudet har blitt bedre i sin rådgivende rolle overfor kommunen gjennom Indigo-samarbeidet.

4.3 Innhentet data: Rutiner og praksis for personvern (kriterie 10)

Dokumentet *Mal-verktøy for utarbeidelse av konsekvensvurdering RSO, viser til at* kommunen gjennomfører avgrensede konsekvensvurderinger innen det som kalles risikostyringsobjektet (heretter kalt RSO-analyser) for IKT-tjenester innenfor tjenesteområdene til Indigo-samarbeidet. [46] RSO-analysen kan typisk gjøres innen en del av et tjenesteområde, et system, en teknisk infrastruktur/komponent/plattform, en prosess, eller et prosjekt. Fagansvarlig fortalte i intervju at arbeidet med RSO-analyser er en relativt ny prosedyre som ble innført av nåværende sikkerhetsansvarlig i Indigo IKT. Videre fortalte hun at det skal utføres RSO-analyse på alt som har med personvern å gjøre.

RSO-analysen følger en skjemabasert prosedyre og består av fem deler; overordnet beskrivelse, ansvarsforhold, sikkerhetsklassifisering av informasjon, sjekkliste om tekniske forhold og konsekvensvurdering. [47] Analysen innebærer blant annet konsekvensvurderinger av realistiske og «verste fall»-scenarioer knyttet til personvernprinsippene konfidensialitet, integritet, og tilgjengelighet. Resultatet av RSO-analysen kan benyttes til å avklare om det skal gjennomføres en risikovurdering (DPIA), eksterne eller interne sikkerhetstester, eller for budsjettmessige vurderinger for å ta høyde for sikkerhetsmessige tiltak.

[45] KOBO er et fagsystem utviklet av Husbanken som brukes til å søke om kommunal bolig.
[46] Stange kommune. *Mal-verktøy for utarbeidelse av konsekvensvurdering RSO*
[47] Stange kommune. *Mal-verktøy for utarbeidelse av konsekvensvurdering RSO*

Revisjonen har fått dokumentasjon fra gjennomførte RSO-analyser ved tre anskaffelser hvor det ble vurdert at man ikke skulle gjennomføre DPIA; en VA-database, et verktøy for gjennomføring av digitale politiske møter, og Smart-TV til undervisning i skolen.

Stange kommune har videre en prosedyre for vurdering av personvernkonsekvenser (DPIA). [48] Hensikten med prosedyren er å dokumentere at kommunen som behandlingsansvarlig har iverksatt tilstrekkelige tiltak for å sikre at behandlingene av personopplysninger er innenfor akseptabel risiko for personvernet til de registrerte. Med hensyn til når DPIA skal gjennomføres, tar prosedyren utgangspunkt i Datatilsynets liste over behandlingsaktiviteter hvor dette er nødvendig. Utover dette skal DPIA også alltid gjennomføres dersom resultatet av en RSO-analyse viser konsekvensnivå Høy eller Svært høy. Videre skal DPIA gjennomføres før oppstart av behandling av helsedata i kombinasjon med bruk av innovativ teknologi, og før bruk av enhver form for kameraovervåkning eller sporingsteknologi. Videre skal behov for DPIA vurderes dersom resultatet av en RSO-analyse viser konsekvensnivå Moderat, eller før behandling av helse- og personopplysninger og ved endringer av behandlinger som kan påvirke sikkerheten.

Prosedyren fastsetter at det ved utarbeidelsen av DPIA alltid skal være minimum tre personer involvert; fagansvarlig, personvernombudet, og en representant fra den aktuelle enheten. [49] Fagansvarlig forklarte i intervju at hvilke ansatte som involveres fra enheten avhenger av hvem som kan faget og skal bruke systemet. Dersom DPIA gjennomføres i samarbeid med andre eierkommuner i Indigo-samarbeidet, er det ikke krav om at kommunens fagansvarlige for informasjonssikkerhet og personvern skal delta. Når det gjelder informasjonssikkerhet og personvern er det veldig mye som gjøres i samarbeid med Indigo IKT og de andre eierkommunene, forklarte fagansvarlige i intervju. Prosedyren beskriver også at det skal tilrettelegges for at representant(er) for de registrerte også kan delta i arbeidet med DPIA.

Fagansvarlig fortalte i intervju at kommunene i Indigo-samarbeidet har et felles DPIA-skjema som skal brukes. Kommunenes prosedyre beskriver at ved utarbeidelse av DPIA skal konsekvenser for den registrerte vurderes når det gjelder hensyn til tilgjengelighet, konfidensialitet, integritet, åpenhet, forutsigbarhet, medbestemmelse og frihet (retten til privatliv m.m.). [50] I tillegg skal robusthet i løsningen vurderes.

Til slutt skal ferdig DPIA signeres og arkiveres i kommunens sak- og arkivsystem.

Revisjonen har fått oversendt dokumentasjon på to gjennomførte DPIA, hvorav begge er utarbeidet av kommunen i samarbeid med andre kommuner. Den første er knyttet til systemet Visma Flyt Samspill (samhandlingsverktøy for koordinering av tverrfaglige tjenester) og er gjennomført av alle kommunene i Indigo-samarbeidet [51], mens den andre er knyttet til systemet Mercell (verktøy for offentlige anskaffelser) og er gjennomført av kommunene Løten, Stange, Ringsaker, Elverum, Lillehammer og Hamar i samarbeid. Utformingen av skjemaene brukt i de to analysene er ulike, men begge skjemaene inneholder; initialvurdering, systematisk beskrivelse, nødvendighet og proporsjonalitet, risikovurdering og restrisikovurderinger etter iverksettelse av tiltak, risikotabell, og sluttrapport med oppsummering av alle vurderinger og tiltak som må/bør iverksettes.

[48] Stange kommune (2025). *DPIA – personvernkonsekvensanalyse - prosedyre*
[49] Stange kommune (2025). *DPIA – personvernkonsekvensanalyse - prosedyre*
[50] Stange kommune (2025). *DPIA – personvernkonsekvensanalyse - prosedyre*
[51] DPIA ble gjennomført før Våler og Åsnes kommuner kom med i Indigo-samarbeidet.

Under gjennomgangen av dokumentasjonen på gjennomførte DPIA fant revisjonen robusthet i løsningen ikke var vurdert i noen av eksemplene. For det andre var ikke punktene som gjelder vurderinger av og synspunkter på behandlingen og dens restrisiko samt ledelsens validering av DPIA fylt ut i rapportfanen. For det tredje var ingen av DPIA-rapportene signert. Revisjonen tok opp dette i intervju med fagansvarlig. Når det gjelder det første punktet, fortalte fagansvarlig at selv om robusthet i løsningen ikke ble vurdert i seg selv, så er innebygd personvern en vesentlig del av kravspesifikasjonen ved IT-anskaffelser. Således er robusthet ifølge den fagansvarlige likevel blitt vurdert. Fagansvarlig hadde ikke noe godt svar på årsaken til de øvrige manglene i eksemplene på gjennomførte DPIA som revisjonen fikk oversendt.

Fagansvarlig fortalte også i intervju at det er planlagt at det skal være en egen modul i Samsvar for gjennomføring av DPIA når de pågående endringsprosessene i Indigo-samarbeidet er ferdig.

4.4 Innhentet data: Behandlingsprotokoll (kriterie 11)

I dokumentbestillingen ba revisjonen om å få oversendt kommunens behandlingsprotokoll. Kommunen oversendte behandlingsprotokollen som ble sendt til Datatilsynet i forbindelse med brevtilsyn i 2023, med forklaring om at de arbeider med å få på plass det nye felles GDPR-systemet (Samsvar) i Indigo-samarbeidet hvor alle behandlingsprotokoller skal være samlet. Dette systemet er ennå ikke ferdigstilt. Behandlingsprotokollen fra 2023 består av 106 ulike behandlinger og er utformet som et standardisert skjema hvor det skal fylles inn følgende informasjon: [52]

- Beskrivelse av dokumentasjonen
- Behandlingens formål
- Lovhjemmel
- Eventuelle unntak
- Behandlingsansvarlig
- Kategori
- Behandlingsgrunnlag
- Slettefrist
- Taushetsplikt
- Sensitive data
- Utført ROS
- Utført DPIA
- Gyldig databehandleravtale
- Type personopplysninger
- Kilde / system
- Databehandler
- Lagring av data
- Informasjon om tekniske sikkerhetstiltak

I intervju spurte revisjonen om hvem som fyller ut behandlingsprotokollene. Fagansvarlig fortalte at hun har fylt ut mange av behandlingsprotokollene. I forbindelse med tilsynet til Datatilsynet i 2023 gjorde de et arbeid med å samle behandlingsprotokollene i et dokument, og da fikk fagansvarlig mye hjelp fra rådgivere i Helse og mestring og i Oppvekst. Fagansvarlig fortalte også at kommunen har fått en betraktelig bedre praksis knyttet til behandlingsprotokoller etter tilsynet i 2023, og at de pågående endringsprosessene i Indigo-samarbeidet vil medføre endringer for hvordan man fører behandlingsprotokoller i kommunen.

Revisjonen stilte også spørsmål ved om det ble gitt noen opplæring i å utarbeide behandlingsprotokoller. Fagansvarlig forklarte i intervju at det ikke er noen opplæring for dette per juni 2025, men at de pågående endringsprosessene i Indigo-samarbeidet vil endre hvordan de fører behandlingsprotokoll i kommunen og at dette inkluderer opplæring i å utarbeide protokoller.

[52] Stange kommune (2023). *Behandlingsprotokoll*

I behandlingsprotokollen revisjonen har fått oversendt er det kun seks av 106 behandlinger hvor feltet om «Slettefrist» er fylt ut. I tilfellene hvor feltet er fylt ut henvises det til lovverk. I intervju forklarte fagansvarlig at dette trolig skyldes at informasjon om slettefrist ikke var et krav da de begynte med den nåværende løsningen for å utarbeide behandlingsprotokoller. Videre fant revisjonen at behandlingene ikke inneholder noe felt som gir informasjon om hvilke mottakere som personopplysningene er blitt eller vil bli utlevert til. I enkelte behandlinger er det imidlertid gitt generelle beskrivelser av dette i «Beskrivelse»-feltet.

Med hensyn til protokoll fra kommunens databehandlere, har revisjonen fått opplyst av kommunen at dette skal foreligge i databehandleravtalene mellom kommunen og deres leverandører. Revisjonen har bestilt et utvalg av kommunens databehandleravtaler (disse er omtalt i kap. 4.6). Under følger beskrivelser av behandlingsprotokoll fra disse databehandleravtalene.

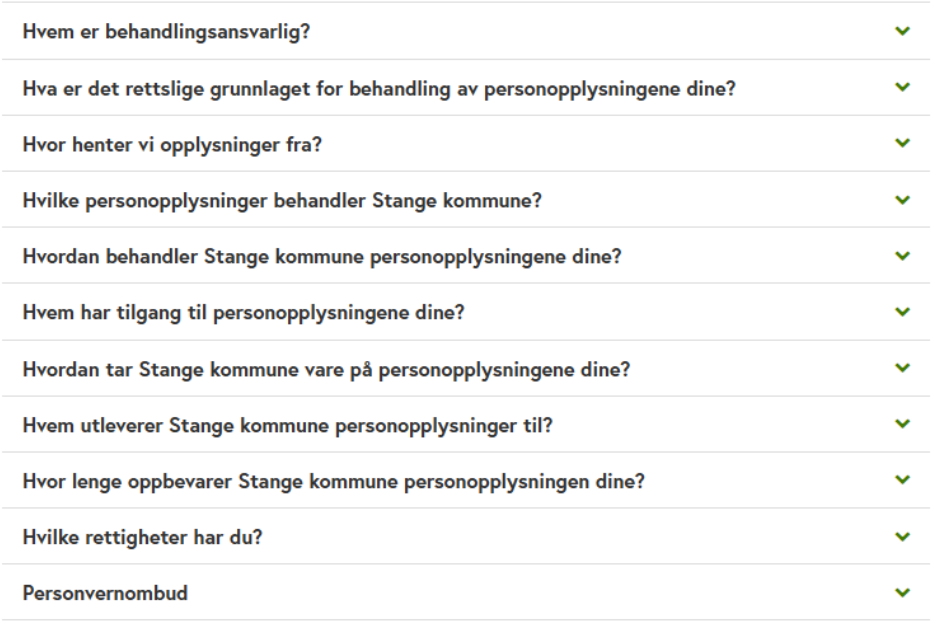
Databehandleravtalen mellom kommunen og Indigo IKT inneholder kontaktinformasjonen til selskapet, daglig leder i selskapet, og fagansvarlig i Stange kommune. Videre inneholder avtalen informasjon om behandlingens formål, karakter, hvilke typer personopplysninger og kategorier av registrerte [53] behandlingen omfatter. Avtalen inneholder også betingelser for overføring av personopplysninger til land utenfor EØS-området (tredjestat) eller til internasjonale organisasjoner. I avtalen finnes også en risikovurdering av behandlingen, samt beskrivelser av spesifikke sikkerhetskrav og tiltak.

Databehandleravtalen mellom kommunen og Visma Flyt AS inneholder kontaktinformasjonen til kommunen og databehandleren. Videre inneholder avtalen informasjon om kategorier av de registrerte og typen personopplysninger som er omfattet av behandlingen, samt kategoriene av behandlinger som utføres på vegne av behandlingsansvarlig. Avtalen inkluderer også en liste med godkjente underleverandører, og betingelser for bruk av eventuelle underleverandører som ikke er omtalt i avtalen. I avtalen er det også beskrevet at databehandleren skal sørge for et høyt sikkerhetsnivå i sine produkter og tjenester gjennom organisatoriske, tekniske, og fysiske sikkerhetstiltak, og at dokumentasjon som angir tiltakene kan oppgis på forespørsel.

4.5 Innhentet data: Personvernerklæring (kriterie 12)

Stange kommune har en personvernerklæring på sin hjemmeside. Personvernerklæringen består av utvidbare seksjoner som man kan klikke på for å åpne og få informasjon om ulike deler av kommunens behandling av personopplysninger (se bildet under). Dette inkluderer informasjon om; behandlingsansvarlig, rettslig grunnlag, innsamling og behandling av personopplysninger, lagring av personopplysningene, hvem som har tilgang til personopplysningene og hvem kommunen utleverer personopplysninger til, den registrertes rettigheter og kontaktinformasjon til personvernombud (se bildet under).

[53] Eksempelvis: Kommunens ansatte, barn og foresatte i barnehagen og grunnskolen, mottakere av voksenopplæring, kommunens innbyggere m.m.



Kilde: Stange kommune sin nettside

Under de utvidbare seksjonene finnes det informasjon om hvilke rettigheter den registrerte har etter personopplysningsloven. Dette gjelder blant annet retten til innsyn, retting, sletting, og protestering. I tillegg er det en egen digital skjemaløsning med BankID-innlogging for henvendelser om den registrertes rettigheter, samt informasjon om alternativer for slike henvendelser dersom man ikke ønsker å bruke den digitale skjemaløsningen.

Under de utvidbare seksjonene gis det også informasjon om hvordan kommunen behandler personopplysninger, deriblant at opplysninger blir overført til elektroniske fagsystemer og brukt til saksbehandling innenfor de ulike virksomhetene. Videre er det beskrevet at opplysningene forblir i fagsystemet inntil den registrerte ikke lenger mottar tjenester eller til saken er ferdig behandlet. Deretter blir opplysningene overført til et digitalt arkiv og lagres i henhold til arkivlovgivningen.

I Stange kommune er ingen avgjørelser knyttet til personopplysninger basert på utelukkende automatisert behandling, forklarte fagansvarlig i intervju.

4.6 Innhentet data: Databehandleravtaler (kriterie 13)

I dialog med kommunen har revisjonen fått opplyst at kommunens databehandleravtaler er samlet i sak- og arkivsystemet ESA. Fagansvarlig fortalte i intervju at de aller fleste avtalene er samlet i en og samme sak i ESA, men at det finnes enkelte som er lagret sammen med kontrakten med leverandøren. På spørsmål om det foreligger databehandleravtaler med alle leverandører, svarte fagansvarlig at dette stort sett er på plass, men at det muligens mangler noe når det gjelder enkelte applikasjoner. Videre fortalte hun at de arbeider med å identifisere, gjennomgå, og legge alle databehandleravtaler inn i Mercell [54] og Samsvar.

[54] Kommunens tjeneste for anskaffelser.

Etter avtale med kommunen har revisjonen gjort et utvalg av kommunens databehandleravtaler for nærmere undersøkelser. Revisjonen har mottatt databehandleravtaler mellom kommunen og følgende leverandører:

- Indigo IKT
    - Selskapet drifter flere av kommunens systemer. Denne avtalen gjelder for følgende systemer; ESA (sak- og arkivsystem), Gerica (fagsystem – helsetjenester), og Sosio (fagsystem – NAV)
- Visma Flyt AS
    - Avtalen gjelder for følgende systemer; Flyt Skole, Flyt Timeplan, Flyt Barnehage, Flyt Sikker Sak skole/barnehage, Flyt Samspill, Flyt Barnevern, Visma Voksenopplæring, Visma HsPro, Visma Flyt Arkiv.

Revisjonen mottok i første omgang en databehandleravtale mellom kommunen og Visma Enterprise AS fra 2018, som gjaldt for fagsystemene i skole og barnehage. Avtalen fra 2018 omfattet ikke fagsystemer knyttet til barneverntjenesten (Flyt Barnevern og Flyt Sikker Sak skole/barnehage), som også er driftet av Visma-konsernet. Revisjonen etterspurte databehandleravtaler knyttet til fagsystemene brukt av barneverntjenesten. I dialog med kommunedirektøren per e-post, beskriver hun at dette er noe kommunen skulle ha fulgt opp i tråd med bestillingen fra revisjonen. Etter at kommunen hadde fått rapporten til høring mottok revisjonen en oppdatert databehandleravtale mellom kommunen og Visma Flyt AS. Denne avtalen ble signert 7. august 2025 og omfatter alle systemene kommunen tar i bruk som er driftet av Visma-konsernet, også det systemene som benyttes av barneverntjenesten.

Under følger en gjennomgang av innholdet i databehandleravtalene som kommunen har oversendt, sett opp mot hva databehandleravtaler skal og bør (full utledning finnes i Vedlegg A) inneholde:

Lovkrav - Personopplysningsloven	Indigo IKT	Visma Flyt AS
Behandling på bakgrunn av instrukser	X	X
Behandlingen er konfidensiell	X	X
Tekniske og organisatoriske sikkerhetstiltak	X	X
Vilkår for underleverandører	X	X
Bistand ved oppfyllelse av de registrertes rettigheter	X	X
Bistand ved sikkerhet og risikovurderinger	X	X
Sletting og/eller tilbakelevering av personopplysninger	X	X
Tilrettelegger for revisjon og inspeksjon	X	X

Anbefalinger - Datatilsynet	Indigo IKT	Visma Flyt AS
Bestemmelser om vederlag og dekning av kostnader	X	X
Krav til tilgangsstyring	X	
Beskrivelse av sikkerhetstiltak i eget vedlegg	X	X
Presisering av ansvar ved bruk av underleverandører	X	
Forventninger til databehandler ved DPIA	X	X
Krav til hvordan sletting spesifikt skal skje	X	
Prosedyre for tilsyn av databehandler i eget vedlegg	X	X
Konkretisering av tilsynsintervall	X	X

4.7 Revisors vurdering

4.7.1 Vurdering av revisjonskriterium 9 – Personvernombud

Undersøkelsen viser at kommunens personvernombud ivaretar de lovpålagte oppgavene som er beskrevet i personvernregelverket, og ombudets oppgaver er klart beskrevet i kommunens oversikt over roller og ansvarsoppgaver i informasjonssikkerhetsarbeidet. I tillegg er kontaktinformasjonen til personvernombudet listet opp i kommunens personvernerklæring. Revisjonen vurderer at personvernombudet i tilstrekkelig grad er gjort kjent for de ansatte i kommunen, og eventuelle andre som har behov for å kontakte ombudet kan enkelt finne kontaktinformasjonen på kommunens nettside.

Vi mener at revisjonskriterium 9 er etterlevd.

Kommunen må ha et personvernombud etter regelverket, og sørge for at personvernombudet er kjent for de ansatte og andre.

4.7.2 Vurdering av revisjonskriterium 10 – Rutiner og praksis for personvern

Kommunen har rutiner for å kontinuerlig kartlegge og identifisere hvilke personopplysninger som blir behandlet gjennom RSO-analyser, samt prosedyrer og verktøy for å gjennomføre vurderinger av personvernkonsekvenser (DPIA) i henhold til personvernlovgivningen. DPIA-prosedyren bidrar til at relevante aktører, som fagansvarlig og kommunens personvernombud, kobles på vurderingene. DPIA-skjemaet utviklet i Indigo-samarbeidet skal videre ivareta at vurderingene skjer i henhold til lovkravene.

Undersøkelsen viser samtidig at flere av feltene i DPIA-skjemaene revisjonen har fått oversendt ikke er fylt ut, og ingen av skjemaene var blitt signert. Kommunen informerer om at man ved innføring av systemet Samsvar vil få på plass en egen DPIA-modul. Vår vurdering er alt i alt at kommunens oppfølging av DPIA-rutinen for personvernkonsekvenser per i dag er noe mangelfull. Dette kan i verste fall øke risikoen for at personvernet ikke i tilstrekkelig grad blir ivaretatt.

Vi mener at revisjonskriterium 10 er delvis etterlevd.

Kommunen må ha nødvendige rutiner, prosedyrer, og praksis som sikrer tilfredsstillende håndtering av personopplysninger, og som oppdateres ved behov.

4.7.3 Vurdering av revisjonskriterium 11 – Behandlingsprotokoll

Revisjonens gjennomgang av kommunens behandlingsprotokoller viser at disse er noe mangelfulle med hensyn til å oppfylle de krav som stilles i personvernregelverket. Spesifikt dreier dette seg om to krav knyttet til den registrertes rett til innsyn. For det første inneholder ikke protokollene informasjon om kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, som eksempelvis kan være databehandlere som behandler personopplysninger på vegne av kommunen. For det andre mangler nesten alle protokollene informasjon om planlagte tidsfrister for sletting av de forskjellige kategoriene for personopplysninger. Dette vurderer revisjonen som uheldig fordi det

kompliserer kommunens evne til å oppfylle den registrertes rett til innsyn, ettersom denne retten innebærer at den registrerte har krav på blant annet denne informasjonen.

Gjennomgangen av databehandleravtalene viser at disse oppfyller alle krav i lovverket med hensyn til at databehandlerne må føre protokoll over kategorier av behandlingsaktiviteter utført på vegne av kommunen. I vår vurdering vil vi likevel vektlegge at revisjonen ikke fikk oversendt gjeldende databehandleravtaler (og dermed behandlingsprotokoll) for fagsystemer knyttet til barneverntjenesten før i august 2025. Revisjonen mener at det knytter seg stor usikkerhet til hvorvidt behandlingsprotokoll for fagsystemene til barneverntjenesten før august 2025 foreligger, noe som er et vesentlig avvik.

Vi mener at revisjonskriterium 11 er delvis etterlevd.

Kommunen må føre protokoller over alle behandlingsaktiviteter.

4.7.4 Vurdering av revisjonskriterium 12 – Personvernerklæring

Kommunen har en omfattende personvernerklæring på sin hjemmeside. Personvernerklæringen er bygd opp av utvidbare seksjoner og er etter revisjonens oppfatning enkel å sette seg inn i.

Revisjonens gjennomgang av personvernerklæringen viser at den inneholder informasjon om den registrertes rettigheter med hensyn til innsyn, retting, sletting, protestering, behandlingsbegrensning, og profilering.

Vi mener at revisjonskriterium 12 er etterlevd.

Kommunen må gi informasjon om hvordan de behandler personopplysninger, gjennom en personvernerklæring.

4.7.5 Vurdering av revisjonskriterium 13 – Databehandleravtaler

Våre undersøkelsen viser at databehandleravtalene revisjonen har fått oversendt oppfyller lovkravene og i stor grad oppfyller anbefalingene fra Datatilsynet. De forbedringspunktene vi fant er knyttet til databehandleravtalen mellom kommunen og Visma Flyt AS. Dette dreier seg om tre momenter; avtalen inneholder ikke krav om at kun autoriserte personer av nødvendige grunner har tilgang til opplysningene, ei heller en presisering om at databehandleren har det fulle ansvaret ovenfor kommunen dersom en underleverandør ikke oppfyller sine forpliktelser etter GDPR, samt krav til hvordan sletting av opplysninger spesifikt skal skje ved avtalens opphør. Alle tre forbedringspunkter er knyttet til Datatilsynets anbefalinger og bidrar til å sikre konfidensiell og trygg behandling av opplysninger, samt bidrar til at kommunen har kontroll på alle opplysninger som den er behandlingsansvarlig for.

Vi mener likevel det er kritikkverdig at kommunen ikke har kunnet oversende gjeldende databehandleravtaler innen revisjonens frister, ikke minst når dette gjelder databehandlere som behandler personopplysninger på vegne av barneverntjenesten som behandler svært sensitiv informasjon. Selv om de avtalene som nå foreligger oppfyller alle lovkrav, påpeker revisjonen at det er usikkert om det har vært noen gjeldende avtaler før august 2025 og at dette er noe kommunen burde ha hatt på plass tidligere.

Vi mener at revisjonskriterium 13 er delvis etterlevd.

Kommunen må sørge for at det foreligger databehandleravtaler med og mellom virksomheter som behandler personopplysninger på vegne av kommunen, og disse må være i henhold til personvernlovgivningen.

5 Konklusjon

Formålet med forvaltningsrevisjonen har vært å undersøke om Stange kommune har en etablert digital sikkerhetskultur som ivaretar internkontroll og avvikshåndtering på en tilfredsstillende måte, samt undersøke i hvilken grad kommunen har rutiner og etablert praksis som sikrer at kommunen oppfyller sine plikter i henhold til personvernregelverket.

For de enkelte problemstillinger kan vi konkludere som følger:

Har Stange kommune etablert en god sikkerhetskultur i organisasjonen, herunder internkontroll og avvikshåndtering?

Revisjonens konklusjon er at Stange kommune alt overveiende har etablert en god sikkerhetskultur i organisasjonen, herunder internkontroll og avvikshåndtering. Kommunen har en tilfredsstillende overordnet informasjonssikkerhetsstrategi samt en sikkerhetsorganisasjon med klare beskrivelser av roller og ansvar i informasjonssikkerhetsarbeidet. Kommunens internkontroll omfatter informasjonssikkerhet, og internkontrollsystemet for informasjonssikkerhet og personvern gjennomgås årlig for å sikre at det fungerer etter hensikten og blir videreutviklet. Kommunen har videre et tilfredsstillende avvikssystem og prosedyrer for håndtering og oppfølging av avvik på informasjonssikkerhetsområdet.

Kommunen har prosedyrer for å gi ansatte relevant opplæring i informasjonssikkerhet og personvern, men har likevel et forbedringspotensial med hensyn til å få ansatte til å gjennomføre slik opplæring. Resultatene fra spørreundersøkelsen indikerer at mange vurderer risikoen som lav, på områder det er knyttet høy risiko til. Samtidig er det en betydelig andel av de ansatte som ikke er kjent med virksomhetens regler for digital sikkerhet. Her konkluderer revisjonen med at kommunen ikke fullt ut har etablert en god nok sikkerhetsatferd blant de ansatte i organisasjonen.

Revisjonen konkluderer at Stange kommune har etablert et rammeverk som tilrettelegger for god sikkerhetskultur, men at det er et forbedringspotensial knyttet til sikkerhetsatferden til de ansatte.

Har Stange kommune etablerte rutiner og praksis som sikrer et tilfredsstillende vern av fysiske personer i forbindelse med behandling av personopplysninger?

Revisjonens konklusjon er at Stange kommune på noen områder har etablert rutiner og praksis som sikrer tilfredsstillende vern av fysiske personer i forbindelse med behandling av personopplysninger. Kommunen har blant annet tilgang på riktig kompetanse på personvernområdet og sikrer at enkeltpersoner får informasjon om kommunens behandling av personopplysninger. Kommunen ivaretar lovpålagte personvernombudstjenester og undersøkelsen viser til at kommunen har en praksis hvor personvernombudet blir involvert når det er relevant. Videre har kommunen utarbeidet en omfattende personvernerklæring som tilrettelegger for at den registrerte kan utøve sine rettigheter etter personvernlovgivningen.

På andre områder konkluderer vi med at kommunen ikke i tilfredsstillende grad har etablert gode nok rutiner og praksis på området. Dette gjelder blant annet med hensyn til gjennomføring av risikovurderinger på personvernområdet (DPIA), og når det gjelder å tydelig kommunisere hva som forventes av den enkelte ansatte med hensyn til digital sikkerhet. Videre har ikke Stange kommune lagt frem gjeldende databehandleravtaler for alle sine systemer innen revisjonens frister, og dermed heller ikke behandlingsprotokoll knyttet til de samme systemene. Per august 2025 har revisjonen fått

dokumentert at dette er kommet på plass, men for enkelte systemer er det usikkert om det har vært noen gjeldende databehandleravtaler før august 2025.

Informasjon vi har mottatt underveis i prosjektet tyder imidlertid på at det er flere prosesser i gang som vil påvirke forbedringspunktene og avvikene. De planlagte endringene i Indigo-samarbeidet vil blant annet innebære at Indigo-kommunene får et felles GDPR-system med Samsvar. I Samsvar vil Indigo-kommunene blant annet kunne gjennomføre DPIA i systemet, samt samle alle databehandleravtaler på ett sted som vil kunne bidra til å gjøre arbeidet med databehandleravtaler mer oversiktlig.

Revisjonen konkluderer at Stange kommune ikke i tilstrekkelig grad har etablerte rutiner og praksis som sikrer et tilfredsstillende personvern ettersom gjeldende databehandleravtaler som er etterspurt ikke er oversendt innen fastsatte frister, og først er kommet på plass per august 2025.

6 Anbefalinger

På bakgrunn av den gjennomførte undersøkelsen anbefaler vi at kommunedirektøren med hensyn til digital sikkerhetskultur og internkontroll bør:

- Sikre at ansatte i større grad gjennomfører kommunens opplæringstiltak på informasjonssikkerhetsområdet.

Og med hensyn til etterlevelse av personvernlovverket anbefaler vi at kommunedirektøren må:

- Sørge for at risikovurderinger av personvernkonsekvenser (DPIA) gjennomføres i henhold til kommunens egne prosedyrer.
- Sørge for at kommunen og kommunens databehandlere systematisk fører protokoll over alle behandlingsaktiviteter.
- Sørge at kommunen har systematiske rutiner for å sikre at det foreligger gjeldende databehandleravtaler knyttet til alle kommunens systemer.
- Sikre at alle ansatte vet hva som forventes av dem med hensyn til digital sikkerhet.

7 Kommunedirektørens uttalelse

Høringsuttalelsen ble oversendt per epost til revisjonen 18. august 2025:

Innledningsvis vil kommunedirektøren påpeke at rapporten oppfattes som grundig og godt gjennomarbeidet. De to problemstillingene som danner grunnlaget for forvaltningsrevisjonen om sikkerhetskultur og internkontroll, og krav vedr. personvernregelverket er svært viktige temaer som kommunedirektøren mener har stor nytteverdi i arbeidet med å utvikle en god sikkerhetskultur.

Det konkluderes i rapporten at Stange kommune alt overveiende har etablert en god sikkerhetskultur i organisasjonen, både i forhold til internkontroll og avvikshåndtering. Videre beskrives det at kommunens informasjonssikkerhetsstrategi også er tilfredsstillende. Dette er meget positivt og viser at det over tid har vært arbeidet systematisk og målrettet med å etablere en digital sikkerhetskultur i Stange kommune. Rapporten påpeker også at det er læringspunkter knyttet til å forbedre og videreutvikle kommunens arbeid. I rapporten framkommer det gode anbefalinger knyttet til forbedringspunkter som kommunedirektøren vil følge opp.

Kommunedirektøren vil i det følgende kommentere de forbedringspunktene som framkommer og beskrive tiltak knyttet til dette.

Problemstilling 1 – sikkerhetskultur, viser rapporten at det er bare ett av åtte punkter som har et forbedringspunkt (gult), kriterium 6. Det handler om at det må iverksettes flere tiltak for opplæring til våre ansatte. Brukerundersøkelsen viser at ansatte ikke i tilstrekkelig grad mener de har fått nok opplæring i informasjonssikkerhet og personvern. Et av kommunens dokumenter, Datavettregler, er laget for at alle ansatte skal få et oversiktlig, forståelig og kortfattet dokument til gjennomlesing. Kommunedirektøren vil i løpet av høsten iverksette tiltak som sikrer at alle ansatte leser dokumentet. Stab for HR – og digitalisering vil gi støtte til implementering avdelingsvis og sørge for at det dokumenteres at ansatte har lest informasjon.

Kontinuerlig opplæring er viktig og nødvendig. Kins (foreningen Kommunal informasjonssikkerhet) kommer med nye opplæringspakker for både ledere og ansatte i løpet av høsten 2025. Når dette foreligger, vil kommunedirektøren initiere at det igangsettes et opplæringsløp for alle ansatte. Opplæringen vil foregå fram til september 2026. I tillegg er det igangsatt arbeid i Indigo-samarbeidet med å utforme et eget opplæringsopplegg for sikkerhetsmåneden i oktober. Arbeid med å lage ferdig et felles styringssystem for informasjonssikkerhet for Indigo-samarbeidet fortsetter utover høsten 2025. Noen dokumenter er allerede klare og i bruk. Det foreligger et gode maler fra Kins som benyttes i dette arbeidet.

Problemstilling 2 – personvern, peker forvaltningsrevisjonen på at tre av fem punkter har forbedringspunkter (gult). Under kriterium nr. 10 – Rutiner og praksis for personvern påpekes det at kommunen delvis har etterlevd dette. Det er riktig som det påpekes i rapporten at det er et pågående arbeid med oppsett av et nytt fagsystem Samsvar, som skal sikre at kommunen har kontroll på all dokumentasjon rundt informasjonssikkerhet. Arbeidet med å innføre denne løsningen vil foregå frem til 1. kvartal 2026.

Kriterium 11 – Behandlingsprotokoll. Her vises det også til at kommunen delvis etterlever dette punktet. Stange kommune var en av mange norske kommuner som fikk brevtilsyn fra Datatilsynet i 2023. I den sammenheng ble det blant annet oversendt oppdatert behandlingsprotokoll. Det gjenstår likevel en del arbeid før vi er i mål. Ved innføring av Samsvar vil kommunen (gjennom Indigo-samarbeidet) identifisere alle behandlinger, kontrakter, databehandleravtaler, ROS og DPIA som er gjennomført i det siste. I den nye løsningen foreligger det egne maler for både gjennomføring av risikovurderinger og DPIA. Arbeidet med dette vil foregå frem til sommeren 2026 før alt er på plass.

Kriterium 13 – Databehandleravtale. Det vises til at oversendte databehandleravtaler oppfyller lovkravene og anbefalingene fra Datatilsynet. Grunnen til at det likevel foreligger forbedringspunkt er at de etterspurte databehandleravtalene først ble sendt til revisjonen etter fristen var utgått. Revisjonen påpeker at det derfor er usikkert om avtalene var på plass før august. Kommunedirektøren har beklaget at avtalene ikke var sendt over i tide. Bakgrunnen for dette var at leverandør valgte å samle flere databehandleravtaler for flere av kommunens fagsystemer inn i en avtale. Denne avtalen ble oversendt i sommer når mange hadde gått i ferie.

Kommunedirektøren vil til slutt takke forvaltningsrevisor for et meget godt samarbeid. Arbeidet har vært gjennomført på en effektivt og grundig måte. Kommunedirektøren har fått tilbakemeldinger fra ansatte, som har vært direkte involvert, om at det har vært et godt samarbeid. Det har vært en lærerik prosess, og nyttig å lese rapporten.

8 Referanser

Internettreferanser

Informasjon om digital sikkerhet på Indigo IKT sin hjemmeside: https://www.indigo-ikt.no/sikkerhet/

Stange kommune sin personvernerklæring: https://www.stange.kommune.no/personvern/

Digdir sin veileder for kartlegging av digital sikkerhetskultur: https://www.digdir.no/informasjonssikkerhet/veileder-kartlegging-av-digital-sikkerhetskultur/2142

Dokumentasjon fra kommunen

Stange kommune (2019). Avtale om kjøp av tjeneste som personvernombud mellom Løten, Stange og Hamar kommuner

Stange kommune (2020). Databehandleravtale mellom Indigo IKT og Visma Enterprise AS

Stange kommune (2021). Sikkerhetsmål og sikkerhetsstrategi

Stange kommune (2022). Databrukeravtale

Stange kommune (2022). Taushetserklæring

Stange kommune (2023). Behandlingsprotokoll

Stange kommune (2023). Helhetlig ROS-analyse 2023-2027

Stange kommune (2023). Informasjonssikkerhet – ledelsens gjennomgang

Stange kommune (2023). Kommuneplan 2023-2025 - Samfunnsdel

Stange kommune (2023). Personopplysningsloven - definisjoner

Stange kommune (2023). Roller, oppgaver og myndighet knyttet til personopplysningsloven

Stange kommune (2023). Sjekkliste for opplæring i GERICA på eget arbeidssted

Stange kommune (2025). Behandling av melding – avvik og hendelser

Stange kommune (2025). Databehandleravtale mellom Stange kommune og Indigo IKT

Stange kommune (2025). Datavettregler

Stange kommune (2025). Dokument hentet fra kommunens kvalitetssystem med signaturer

Stange kommune (2025). DPIA – personvernkonsekvensanalyse - prosedyre

Stange kommune (2025). Informasjonssikkerhet og personvern - Opplæringsskriv

Stange kommune (2025). Introduksjonsplan nyansatte helse- og omsorgssenter - sjekkliste

Stange kommune (2025). Meldeplikt - oversikt

Stange kommune (2025). Melding av hendelser, avvik og skademelding - prosedyre

Stange kommune (2025). Powerpoint-presentasjon og møtereferat fra ledelsens gjennomgang for informasjonssikkerhet 2025

Stange kommune. Mal-verktøy for utarbeidelse av konsekvensvurdering RSO

Vedlegg A: Revisjonskriterier

Om utledningen av revisjonskriterier

Revisjonskriterier er de krav, normer og/eller standarder som den reviderte enheten skal bli vurdert i forhold til. Utgangspunktet for revisjonskriteriene er problemstillingene, og det skal være utledet revisjonskriterier for hvert forvaltningsrevisjonsprosjekt.

Kriteriene skal utledes fra autoritative og anerkjente kilder innenfor det reviderte området. Slike kilder kan være lover, forskrifter, forarbeider, rettspraksis, politiske vedtak, mål og føringer, administrative retningslinjer, statlige føringer, veiledere og lignende, andre myndigheters praksis, anerkjent teori og reelle hensyn.

Kriteriene skal være relevante, konkrete og i samsvar med kravene som gjelder for den reviderte enheten i den aktuelle tidsperioden for revisjonen. Den reviderte enheten skal presenteres for kildene til kriteriene og gis anledning til å komme med innspill.

Vi velger å sende revisjonskriteriene i sin helhet over til revidert enhet, slik at kravene kommer tydelig frem og det blir enklere å komme med konkrete tilbakemeldinger. Vi tar forbehold om at kriteriene kan bli endret eller at ikke alle fremsatte kriterier vil bli vurdert.

Bakgrunn for bestillingen

Kontrollutvalget i Stange kommune behandlet prosjektplan om digital sikkerhetskultur og personvern i møte den 14. oktober 2024 (sak 45/24). På bakgrunn av prosjektplanens forslag til formål og problemstillinger, fattet kontrollutvalget følgende vedtak:

> Vedtak, enstemmig:
> Kontrollutvalget godkjenner revisors prosjektplan innen forvaltningsrevisjon av personvern og IKT under følgende forutsetninger:
> a) Kontrollutvalgets merknader og innspill som fremkom i møte tas med i det videre arbeidet
> b) Kommunestyrets godkjennelse av kontrollutvalgets plan for forvaltningsrevisjon og eierskapskontroll i kommunestyrets møte 23. oktober 2024.

Kontrollutvalgets innspill til prosjektplanen omhandlet avvikskultur og sikkerhetsdefinisjoner, nærmere bestemt om det er en felles forståelse for avvik i organisasjonen og om kommuneledelsen har kommunisert felles sikkerhetsdefinisjoner nedover i organisasjonen slik at alle ansatte forstår sikkerhet på samme måte. Begge innspillene mener vi belyses innenfor de kriteriene som er utledet.

I møte den 23. oktober 2024 vedtok kommunestyret kontrollutvalgets plan for forvaltningsrevisjon og eierskapskontroll for Stange kommune i perioden 2024-2028, jf. sak 81/24.

Utledning av revisjonskriterier

Utledning av revisjonskriterier for problemstilling 1

Har Stange kommune etablert en god sikkerhetskultur i organisasjonen, herunder internkontroll og avvikshåndtering?

Overordnet mål og strategi (Kriterie 1-3)

Etter kommuneloven § 25-1 skal kommunedirektøren sørge for å ha et system for internkontroll som sikrer at lover og forskrifter følges i hele kommunens virksomhet. [55] Dette innebærer:

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

KS har utarbeidet en veileder for hvordan kommunen kan arbeide systematisk med internkontrollen. Arbeidet kan oppsummeres i følgende modeller: [56]

Figur 1. Som figurene viser innebærer internkontroll med andre ord at kommunen må ha systemer for å planlegge, utføre, kontrollere, og korrigere sin virksomhet. Videre viser modellene blant annet til at risikovurderingene er et viktig grunnlag både for internkontroll og tiltak både på strategisk og operativt nivå.

Internkontrollbestemmelsen er generell og gjeldende for alt kommunen har av virksomhet. I og med at informasjonssikkerhet er et svært viktig område som følge av at mye av offentlig virksomhet er avhengig av digitale informasjonssystemer, er det stilt særskilt krav til internkontroll innen informasjonssikkerhet i eForvaltningsforskriften. Det følger av forskriftsbestemmelsene at forvaltningsorganer som benytter elektronisk kommunikasjon skal ha: [57]

- Beskrevet mål og strategi for informasjonssikkerhet i virksomheten – dvs. sikkerhetsmål og sikkerhetsstrategi.
- Mål og strategiene skal legges til grunn for internkontrollen.
- Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

[55] Kommuneloven § 25-1. *Internkontroll i kommunen og fylkeskommunen*.
[56] KS 2020. *Orden i eget hus: Kommunedirektørens internkontroll*.
[57] eForvaltningsforskriften § 15. *Internkontroll på informasjonssikkerhetsområdet*.

- Internkontrollen skal være basert på anerkjente standarder for styringssystem for informasjonssikkerhet.
- Omfang og innretning skal være tilpasset risiko og bør integreres som en del av virksomhetens helhetlige styringssystem.

Det finnes mange anerkjente standarder for et styringssystem for informasjonssikkerhet. Den mest nærliggende å se til for kommunal sektor er KS sin veileder for personvern og informasjonssikkerhet. [58]

Veilederen viser til de fire aktivitetene planlegge, utføre, kontrollere og korrigere, basert på Demings sirkel som vist i figur 1.

Innen **planlegging**, fremgår det at kommunen bør skaffe oversikt over sentrale informasjonsverdier og vurdere hvor kritiske de er for kommunens drift og tjenesteproduksjon. Dette inkluderer en oversikt over behandling av personopplysninger.

Som en del av planleggingen beskriver veilederen videre at kommunen som et minimum bl.a. bør fastsette og dokumentere hvem som har ansvar for:

- Å føre oversikt over informasjonsverdier.
- Vurdering av kritikalitet.
- Vedlikehold av behandlingsprotokoll.
- Gjennomføring av risikovurderinger.
- Gjennomføring av personvernkonsekvensvurderinger.
- Oppfølging av eksterne leverandører.
- Å stille krav til eksterne leverandører.

Det må gjennomføres risikovurderinger og på bakgrunn av denne utarbeides en tiltaksplan med oversikt over hvem som er ansvarlig for tiltakene som skal gjennomføres.

Vi legger til grunn at kommunen må ha utarbeidet sikkerhetsmål og en sikkerhetsstrategi for informasjonssikkerhet, og at kommunen har en sikkerhetsorganisasjon med beskrivelser av ansvar og roller for informasjonssikkerhetsarbeidet. I tillegg legger vi til grunn at kommunen må ha oversikt over sentrale informasjonsverdier, samt hvor kritiske disse er for kommunens drift og tjenesteproduksjon.

Internkontroll på informasjonssikkerhet- og personvernområdet (Kriterie 4-6)

Når det gjelder krav til **utføring** som en del av kommunens styringssystem, anbefales kommunene å utforme, innføre og gjennomføre fastsatte internkontrollaktiviteter, slik at denne fremstår systematisk. Som et minimum, nevner KS-veilederen blant annet at det å utføre bør innebære følgende aktiviteter: [59]

- Overordnet beskrivelse av kommunens sikkerhetsbehov.
- Organisering av arbeidet, herunder roller og ansvar for sikkerhet og personvern.
- Hvordan og hvor kommunen skal føre oversikt over informasjonsverdier og behandling av personopplysninger.
- Sikrer at IKT og personvern er en del av kommunens kontinuitets- og beredskapsplan.
- Hvordan kommunen skal ivareta personvernet og de registrertes rettigheter, bl.a.
    - Utarbeide og vedlikeholde personvernerklæring

[58] KS 2022. *Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet*.
[59] Ibid: 28

    - Forespørsel om innsyn, retting og sletting
    - Ivaretakelse av personvernprinsippene
- Hva som skal gjøres ved en ny behandling av personopplysninger og innføring av nye IKT-systemer.
- Hvordan kommunen skal arbeide med kompetanse og opplæring knyttet til personvern og informasjonssikkerhet.
- Hvordan kommunen skal jobbe med tilgangskontroll til systemer og informasjon.
- Når og hvordan det skal gjennomføres risikovurderinger og personvernkonsekvensvurderinger.
- Hvilke krav som stilles til IKT-systemer og leverandører, og hvordan de følges opp.
- Håndtering av avvik knyttet til personvern og informasjonssikkerhet.

Med hensyn til punktet **kontroll** i Demings sirkel, blir det anbefalt at kommunen ivaretar aktiviteter som i hovedsak har to funksjoner: [60]

- At de definerte internkontrollaktivitetene gjennomføres og fungerer som forutsatt.
- At de bidrar til videreutvikling av internkontrollen.

Det sistnevnte punktet inkluderer at kommunen har et system for å identifisere og følge opp nye eller endrede krav, oppdatere rutiner og instrukser, oppdatere oversikt over informasjonsverdier, oppdatere oversikt over personopplysningsbehandlinger, oppdatere risikovurderinger mv.

Kommunens ledelse bør minimum en gang i året gjennomgå personvern og informasjonssikkerhet. Formålet er å gå gjennom status, slik at kommunedirektøren får tilstrekkelig informasjon om risikoer knyttet til informasjonssikkerhet og personvern, og enklere kan ta avgjørelser for å iverksette nødvendige tiltak og forbedringer.

Kommunen bør føre egenkontroll gjennom vurdering og evaluering av praksis og kontrollere for om internkontrollen fungerer etter hensikten. Egenkontrollen bør være risikobasert og ha ulike temaer for hver gang den gjennomføres.

Vi legger til grunn at kommunens internkontroll omfatter informasjonssikkerhet og personvern, og at systemet for internkontroll på informasjonssikkerhet- og personvernområdet bør gjennomgås årlig. Videre mener vi at internkontrollsystemet må ivareta kravene i personvernlovgivningen. I tillegg legger vi til grunn at kommunen må ha tiltak som sikrer opplæring for ansatte innen informasjonssikkerhet.

Avvikshåndtering (Kriterie 7-8)

Innen **korrigering** blir det anbefalt at kommunens erfaringer fra og innsikt i hva som fungerer og ikke fungerer i utførings- og kontrollfasen, over tid benyttes til forbedringer og oppfølging av svakheter i kommunens system for informasjonssikkerhet og personvern. [61]

I dette ligger blant annet avviksregistrering og -håndtering, og evaluering og læring av innmeldte feil, særlig de som er systematiske – enten ved at feilene gjentas eller at feilene ligger fundamentalt til bestemte praksiser.

Vi legger til grunn at kommunen må ha et system for avviksregistrering for informasjonssikkerhets- og personvernområdet. Vi mener videre at kommunen må gjennomgå og håndtere avvik, slik at de kan

[60] Ibid: 29
[61] Ibid: 31

brukes til forbedringsarbeid i prosedyrer og praksis for ivaretakelsen av informasjonssikkerhet og personvern.

Punktvis oppsummering av revisjonskriterier for problemstilling 1

Utledningen av krav og forventninger til kommunens arbeid med å skape en god sikkerhetskultur kan oppsummeres i følgende punkter:

1. Kommunen må ha utarbeidet sikkerhetsmål og en sikkerhetsstrategi, og strategien må være kjent for de ansatte.
2. Kommunen må ha en sikkerhetsorganisasjon med beskrivelser av ansvar og roller for informasjonssikkerhet.
3. Kommunen må ha skaffet oversikt over sentrale informasjonsverdier og hvor kritiske disse er for kommunens drift og tjenesteproduksjon.
4. Kommunen må ha en internkontroll som omfatter informasjonssikkerhet og personvern, herunder etablere aktiviteter som sikrer at internkontrollen gjennomføres og fungerer som forutsatt.
5. Systemet for internkontroll innen informasjonssikkerhet og personvern bør gjennomgås årlig.
6. Kommunen må ha tiltak som sikrer at ansatte får opplæring knyttet til informasjonssikkerhet og personvern.
7. Kommunen må ha et system for avviksregistrering innenfor informasjonssikkerhet og personvern.
8. Avvik må gjennomgås, håndteres, og brukes for forbedring av prosedyrer og praksis i ivaretakelsen av informasjonssikkerhet og personvern.

Utledning av revisjonskriterier for problemstilling 2

Har Stange kommune etablerte rutiner og praksis som sikrer et tilfredsstillende vern av fysiske personer i forbindelse med behandling av personopplysninger?

Personopplysningsloven og personvernforordningen (GDPR) beskriver en rekke grunnleggende prinsipper for behandling av personopplysninger (personvernprinsippene) og stiller noen krav til hva kommunen må ha på plass for å sikre den enkeltes personvern. Det følgende er en utledning av personvernprinsippene og lovkravene knyttet til personvern. I utledningen har vi valgt å bruke begrepene *behandlingsansvarlig* og *databehandler* slik som i lovverket. Den behandlingsansvarlige er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal benyttes, og vil i denne sammenhengen være kommunen. En databehandler er en som behandler personopplysninger på vegne av andre. Dette kan være en fysisk eller juridisk person, offentlig myndighet, institusjon, eller annet organ, men som regel være en ekstern virksomhet eller enhet. Databehandleren behandler alltid personopplysninger etter instruks fra en annen virksomhet (den behandlingsansvarlige). [62]

Personvernprinsippene og personvernombud (Kriterie 9)

Personvernprinsippene i GDPR artikkel 5 slår fast at personopplysninger skal: [63]

a) behandles på en lovlig, rettferdig, og åpen måte med hensyn til den registrerte,

[62] Datatilsynet - Behandlingsansvarlig og databehandler

[63] Personopplysningsloven, personvernforordningen. *Artikkel 5. Prinsipper for behandling av personopplysninger pkt. 1*.

b) samles inn for spesifikke, uttrykkelig angitte, og berettigede formål,
c) være adekvate, relevante, og begrenset til det som er nødvendig for formålene de behandles for,
d) være korrekte og om nødvendig oppdaterte,
e) lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for,
f) behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene.

Personvernprinsippene skal sikre at behandling av personopplysninger skjer på en måte som i størst mulig grad sikrer forutsigbarhet og forholdsmessighet for enkeltmennesket. Datatilsynet har, på bakgrunn av punktene i lovteksten, oppsummert personvernprinsippene på følgende måte: [64]

- Lovlig, rettferdig, og åpen/gjennomsiktig
  - Det må finnes et rettslig grunnlag for planlagt behandling av personopplysninger, behandlingen av personopplysninger skal gjøres i respekt for den registreres interesser og være forståelig for de registrerte, i tillegg skal bruken av personopplysninger være oversiktlig og forutsigbar for personen opplysningene gjelder.
- Formålsbegrensning
  - Personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte, og legitime formål. Dette innebærer at ethvert formål med behandling av personopplysninger skal identifiseres og beskrives presist, samt være forklart på en slik måte at alle berørte personer kan forstå hva personopplysningene skal brukes til.
- Dataminimering
  - Mengden av innsamlede personopplysninger skal begrenses til det som er nødvendig for å realisere formålet med innsamlingen.
- Riktighet
  - Personopplysninger som behandles skal være korrekte, og om nødvendig skal de oppdateres. Dette innebærer at den behandlingsansvarlige må sørge for å straks slette eller rette personopplysninger som er uriktige.
- Lagringsbegrensning
  - Prinsippet om lagringsbegrensning innebærer at personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for.
- Integritet og konfidensialitet
  - Personopplysninger skal behandles slik at opplysningenes integritet, konfidensialitet, og tilgjengelighet beskyttes. Dette innebærer at den behandlingsansvarlige må sørge for å iverksette tiltak mot utilsiktet og ulovlig ødeleggelse, tap, og endringer av personopplysninger.
- Ansvarlighet
  - Prinsippet om ansvarlighet innebærer at virksomheter som behandler personopplysninger må vise at man tar ansvar for å opptre i samsvar med personvernprinsippene. Dette betyr at virksomheten må kunne dokumentere at den har gjennomført tiltak for å etterleve personvernforordningen, og at virksomheten må opptre proaktivt og etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid.

[64] Datatilsynet - Personvernprinsippene

Kommunen, som behandlingsansvarlig, er ansvarlig for at personvernprinsippene overholdes ved behandling av personopplysninger. [65]

Kommunen skal, som en offentlig myndighet, utpeke et personvernombud. [66] Personvernombudet skal utpekes på grunnlag av faglige kvalifikasjoner, kunnskap om personvernlovgivning, og evne til å utføre vervets oppgaver. Det er kommunen selv som skal vurdere om en person er kvalifisert til å være personvernombud. [67] Europakommisjonen har utgitt retningslinjer som forklarer mer om krav til faglige kvalifikasjoner, ekspertise, og evner for personvernombud.

Videre i personvernforordningen er det beskrevet at den behandlingsansvarlige og databehandleren skal sikre at personvernombudet på riktig måte og i rett tid involveres i alle spørsmål som gjelder vern av personopplysninger. [68] Personvernombudet skal få støtte, ressurser, og tilganger som er nødvendig for å utføre sine oppgaver. Den behandlingsansvarlige skal sikre at personvernombudet har en uavhengig rolle og kan utføre sine funksjoner og oppgaver på en uavhengig måte. Personvernombudet kan utføre andre oppgaver og ha andre plikter, men den behandlingsansvarlige må sikre at nevnte oppgaver eller plikter ikke fører til en interessekonflikt.

Når det gjelder personvernombudets oppgaver beskriver personvernforordningen at disse i det minste skal omfatte: [69]

- Å informere og gi råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har i henhold til personvernforordningen.
- Å kontrollere overholdelsen av personvernforordningen og den behandlingsansvarliges eller databehandlerens personvernretningslinjer, herunder fordeling av ansvar, holdningsskapende tiltak og opplæring av personellet som er involvert i behandlingsaktivitetene, og tilhørende revisjoner.
- På anmodning gi råd om vurderingen av personvernkonsekvenser og kontrollere gjennomføring av den.
- Samarbeide med og fungere som kontaktpunkt med tilsynsmyndigheten.

Vi legger til grunn at kommunen må ha et personvernombud som fungerer i henhold til personvernlovgivningen.

Risikovurderinger for behandlinger (Kriterie 10)

I tilfeller hvor det er sannsynlig at behandlingen av personopplysninger vil medføre en risiko for fysiske personer sine rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet (DPIA). [70] En DPIA [71] er en prosess for å sikre og dokumentere at den behandlingsansvarlige vil kunne etterleve kravene etter personvernforordningen der behandlingen av personopplysninger kan innebære en høy risiko for de registrerte. Den behandlingsansvarlige skal rådføre seg med personvernombudet ved utføringen av en DPIA.

[65] Personopplysningsloven, personvernforordningen. *Artikkel 5. Prinsipper for behandling av personopplysninger pkt. 2*.
[66] Personopplysningsloven, personvernforordningen. *Artikkel 37. Utpeking av et personvernombud, pkt. 1*.
[67] Olsen, T. (2024, 30. september) *Norsk lovkommentar: Personopplysningsloven, note 420.* Rettsdata.no
[68] Personopplysningsloven, personvernforordningen. *Artikkel 38. Personvernombudets stilling*.
[69] Personopplysningsloven, personvernforordningen. *Artikkel 39. Personvernombudets oppgaver, pkt. 1*.
[70] Personopplysningsloven, personvernforordningen. *Artikkel 35. Vurdering av personvernkonsekvenser, pkt. 1*.
[71] Fra den engelske betegnelsen: «Data Protection Impact Assessment».

Datatilsynet har laget en veiledning som gir oversikt over når en DPIA skal gjennomføres, hvem som har ansvaret for gjennomføringen, og i hvilke situasjoner det ikke er nødvendige å gjennomføre en DPIA. [72] Datatilsynet har satt sammen en liste med eksempler på når en DPIA skal gjennomføres, men denne er ikke uttømmende og det kan foreligge høy risiko ved behandlingsaktiviteter som ikke omfattes av listen. Videre anbefaler Datatilsynet at det gjennomføres en DPIA i tilfeller hvor det er usikkert om det er nødvendig å gjøre det, ettersom det er et nyttig verktøy for å sikre at personvernforordningen følges. Følgende behandlingsaktiviteter krever alltid at det gjennomføres en DPIA: [73]

- Personopplysninger samlet inn via en tredjepart i følge med minst ett annet kriterium.
    - For eksempel innsamling og sammenstilling av personopplysninger fra tredjeparter for å avgjøre om den registrerte skal få tilbud om, fortsette å motta, eller nektes et produkt, en tjeneste, eller et tilbud.
- Behandling av personopplysninger med innovativ teknologi i følge med minst ett annet kriterium.
    - For eksempel behandling av helseopplysninger med innovativ velferdsteknologi som helseimplantater.
- Behandling av personopplysninger for systematisk monitorering av ansatte.
    - For eksempel overvåking av ansattes internettaktivitet, elektroniske kommunikasjon, og kameraovervåkning.
- Behandling av personopplysninger, uten samtykke, for vitenskapelige eller historiske formål i følge med minst ett annet kriterium.
    - For eksempel behandling av helseopplysninger for forskningsformål uten den registrertes samtykke.
- Behandling av personopplysninger for å evaluere læring, mestring, og trivsel i skoler eller barnehager.
- Systematisk monitorering, inkludert kameraovervåkning, på offentlig tilgjengelige områder i stor skala.
- Kameraovervåkning i skoler og barnehager i åpningstider.
- Behandling av personopplysninger ved å systematisk monitorere effektivitet, ferdigheter, kunnskap, mental helse, og utvikling.
- Innsamling av personopplysninger i stor skala gjennom «tingenes internett» eller velferdsteknologi.

Følgende er en oversikt over noen situasjoner der det anses at det ikke krever en DPIA:

- Dersom behandlingen sannsynligvis ikke «vil medføre en høy risiko».
- Dersom behandlingens art, omfang, sammenheng og formål er veldig lik en behandling det allerede er gjennomført en DPIA for. I slike situasjoner kan resultatet fra den foreliggende vurderingen for lignende behandlinger brukes.
- Dersom en behandling er i samsvar med artikkel 6 nr. 1 bokstav c [74] eller bokstav e [75] *og* har et rettsgrunnlag etter EU-retten eller nasjonal lovgiving, der tilhørende lovgivning regulerer den spesifikke behandlingen og en DPIA allerede er gjennomført som ledd i utarbeidelse av rettsgrunnlaget.

[72] Datatilsynet – Vurdering av personvernkonsekvenser (DPIA)
[73] Vi har plukket ut punktene som er relevante for kommunen. Hele listen er å finne her.
[74] Behandlingen av personopplysninger er nødvendig for å oppfylle en rettslig forpliktelse.
[75] Behandlingen av personopplysninger er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet.

For å vurdere om en behandlingsaktivitet medfører høy risiko for at de registrertes rettigheter etter personvernforordningen ikke ivaretas, kan man bruke Artikkel 29-gruppens [76] kriterier for å vurdere behov for DPIA. I de fleste situasjoner kan en behandlingsansvarlig anta at det skal utføres en DPIA dersom minst to av følgende ni kriterier er oppfylt: [77]

1. Evaluering eller poengsetting.
    - Aspekter som gjelder arbeidsprestasjoner, økonomisk situasjon, helse, personlige preferanser eller interesser, pålitelighet eller atferd, plassering eller bevegelser.
2. Automatisk beslutninger med rettslig eller tilsvarende betydelig virkning.
    - Behandling som har som formål å ta beslutninger om den registrerte som har rettsvirkning for den fysiske personen eller på lignende måte i betydelig grad påvirker den fysiske personen.
3. Systematisk monitorering.
    - Behandlingsaktiviteter som brukes for å observere, overvåke eller kontrollere de registrerte, inkludert opplysninger som har blitt samlet inn gjennom nettverk eller systematisk overvåking i stor skala av et offentlig tilgjengelig område.
4. Særlige kategorier av personopplysninger eller opplysninger av svært personlig karakter.
    - Kategorier av personopplysninger tidligere kalt sensitive personopplysninger som er definert i artikkel 9 i personvernforordningen, samt personopplysninger vedrørende straffedommer og lovovertredelser som definert i artikkel 10 i personvernforordningen.
5. Personopplysninger behandles i stor skala.
6. Matching eller sammenstilling av datasett.
    - Dette kan for eksempel stamme fra to eller flere databehandlingsoperasjoner som gjennomføres med ulike formål og/eller av ulike behandlingsansvarlige på en måte som overstiger den registrertes rimelige forventninger.
7. Personopplysninger om sårbare registrerte.
    - Omfatter personopplysninger knyttet til enkeltpersoner som kan være ute av stand til, og på en enkel måte, å gi sitt samtykke eller motsette seg behandlingen av sine personopplysninger eller utøve sine rettigheter. Sårbare registrerte kan omfatte barn, arbeidstakere, psykisk syke personer, asylsøkere, eldre personer, pasienter osv., samt i de situasjoner der det foreligger en ubalanse i forholdet mellom den registrerte og den behandlingsansvarlige.
8. Innovativ bruk eller anvendelse av ny teknologisk eller organisatorisk løsning.
    - De personlige og sosiale konsekvensene ved anvendelsen av ny teknologi kan være ukjente. En DPIA hjelper den behandlingsansvarlige å forstå og håndtere slike risikoer. For eksempel kan visse «tingenes internett»-applikasjoner [78] få betydelige konsekvenser for den enkeltes dagligliv og privatliv.
9. Når behandlingen «hindrer de registrerte i å utøve en rettighet eller gjøre bruk av en tjeneste eller en avtale».
    - Omfatter behandlinger som tar sikte på å tillate, endre eller nekte den registrerte tilgang til en tjeneste eller inngå en avtale. For eksempel når en bank kredittvurderer sine kunder mot en database for å avgjøre om de skal tilbys lån.

[76] Artikkel 29-gruppen er en rådgivende arbeidsgruppe innenfor EU, som består av representanter fra EU-landenes nasjonale datatilsyn. Datatilsynet i Norge deltar i gruppen som observatør uten stemmerett.
[77] Datatilsynet – Vurdering av personvernkonsekvenser (DPIA): Når er det høy risiko?
[78] «Tingenes internett» refererer til fysiske enheter som kan kommunisere med hverandre og med internett, eksempelvis bilder, klokker, overvåkningsutstyr, låsemekanismer m.m.

Desto flere av disse kriteriene en behandlingsaktivitet oppfyller, desto mer sannsynlig er det at det foreligger en høy risiko. Det er derfor et krav om å gjennomføre en DPIA, uavhengig av hvilke tiltak den behandlingsansvarlige har planer om å iverksette. Dersom den behandlingsansvarlige vurderer at behandlingsaktiviteten ikke vil medføre en høy risiko, og at det derfor ikke er et behov for å gjennomføre en DPIA, så bør den behandlingsansvarlige begrunne og dokumentere hvorfor en DPIA ikke gjennomføres. I denne dokumentasjonen bør personvernombudets synspunkter inkluderes.

Når det gjelder innholdet i en DPIA, så er det beskrevet i personvernforordningen at denne i det minste skal inneholder: [79]

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, 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.

I tillegg skal den behandlingsansvarlige innhente synspunkter på den planlagte behandlingen fra de registrerte eller deres representanter dersom det er relevant, uten at det berører vernet av kommersielle eller allmenne interesser eller sikkerheten ved behandlingsaktivitetene. [80] Praktisk sett kan dette innhentes gjennom en forening eller lignende som representerer de registrerte. Dersom den behandlingsansvarlige sin beslutning avviker fra synspunktene til de registrerte, bør det fremgå av vurderingen hvorfor beslutningen likevel treffes. [81]

Vi legger til grunn at kommunen må gjennomføre en vurdering av personvernkonsekvenser (DPIA) før behandlingen av særlig sensitive personopplysninger i henhold til personvernlovgivningen, og at disse er skriftlig dokumentert. Dette innebærer også at man kartlegger og identifiserer hvilke personopplysninger kommunen har.

Behandlingsprotokoller (Kriterie 11)

Den behandlingsansvarlige (eller den behandlingsansvarliges representant) skal føre en protokoll over behandlingsaktiviteter som utføres (behandlingsprotokoll). Behandlingsprotokollen skal inneholde følgende informasjon: [82]

a) Navnet på og kontaktopplysningene til den behandlingsansvarlige og, dersom det er relevant, den felles behandlingsansvarlige, den behandlingsansvarliges representant og personvernombudet.
b) Formålene med behandlingen.
c) En beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger.
d) Kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, herunder mottakere i tredjestater eller internasjonale organisasjoner.

[79] Personopplysningsloven, personvernforordningen. *Artikkel 35. Vurdering av personvernkonsekvenser, pkt. 7*.
[80] Personopplysningsloven, personvernforordningen. *Artikkel 35. Vurdering av personvernkonsekvenser, pkt. 9*.
[81] Olsen, T. (2024, 30. september) Norsk lovkommentar: Personopplysningsloven, note 403. Rettsdata.no
[82] Personopplysningsloven, personvernforordningen. *Artikkel 30. Protokoller over behandlingsaktiviteter, pkt. 1*

e) Dersom det er relevant, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon, herunder identifikasjon av nevnte tredjestat eller internasjonale organisasjon.
f) Dersom det er mulig, de planlagte tidsfristene for sletting av de forskjellige kategoriene av opplysninger.
g) Dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i GDPR artikkel 32, pkt 1.

Videre skal hver databehandler (eller databehandleres representant) føre en protokoll over alle kategorier av behandlingsaktivitetene som er utført på vegne av en behandlingsansvarlig, og som skal inneholde: [83]

a) Navnet på og kontaktopplysningene til databehandleren eller databehandlerne og til hver behandlingsansvarlig som databehandleren opptrer på vegne av, samt, dersom det er relevant, den behandlingsansvarliges eller databehandlerens representant og personvernombudet.
b) Kategoriene av behandling utført på vegne av hver behandlingsansvarlig.
c) Dersom det er relevant, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon, herunder identifikasjon av nevnte tredjestat eller internasjonale organisasjon.
d) Dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i GDPR artikkel 32, pkt 1.

Behandlingsprotokollene nevnt over skal være skriftlige og elektroniske. [84] Det er ingen formkrav til hvordan behandlingsprotokollene skal føres, men Datatilsynet har utarbeidet maler til både behandlingsansvarlig og databehandler på sin nettside. [85] Disse malene inneholder flere punkter enn det som er obligatorisk etter lovverket, men som vil gjøre det lettere å besvare forespørsler fra enkeltpersoner som ønsker å vite hva kommunen har registrert om dem, hvor kommunen har fått opplysningene fra, og med hvilket rettslig grunnlag kommunen har behandlet opplysningene.

Vi legger til grunn at kommunen utarbeider behandlingsprotokoller i henhold til personvernlovgivningen, og at databehandlere som behandler personopplysninger på vegne av kommunen utarbeider behandlingsprotokoller med oversikt over behandlingsaktivitetene som er gjennomført etter instruks fra kommunen.

Personvernerklæring (Kriterie 12)

For å overholde personvernprinsippet om åpenhet og rettferdighet skal den behandlingsansvarlige sørge for at den registrerte får informasjon om behandlingen av personopplysninger på en kortfattet, åpen, forståelig, og lett tilgjengelig måte. [86] I tillegg skal den behandlingsansvarlige tilrettelegge for at den registrerte kan utøve sine rettigheter med hensyn til innsyn, retting og sletting, begrensning av behandling, dataportabilitet, protestering, og profilering. [87] Vanligvis skjer dette gjennom en personvernerklæring, og det anbefales at denne er kortfattet og forståelig.

[83] Personopplysningsloven, personvernforordningen. *Artikkel 30. Protokoller over behandlingsaktiviteter, pkt. 2*
[84] Personopplysningsloven, personvernforordningen. *Artikkel 30. Protokoller over behandlingsaktiviteter, pkt. 3*
[85] Datatilsynet - Protokoll over behandlingsaktiviteter
[86] Personopplysningsloven, personvernforordningen. *Artikkel 12. Klar og tydelig informasjon, kommunikasjon og nærmere regler om utøvelse av den registrertes rettigheter, pkt. 1*.
[87] Personopplysningsloven, personvernforordningen. *Artikkel 12. Klar og tydelig informasjon, kommunikasjon og nærmere regler om utøvelse av den registrertes rettigheter, pkt. 2*.

Vi legger til grunn at kommunen sikrer at enkeltpersoner får informasjon om kommunens behandling av personopplysninger på en forståelig og lett tilgjengelig måte, gjennom en personvernerklæring. Videre mener vi at denne skal inkludere informasjon om hvordan den registrerte kan utøve sine rettigheter etter personvernlovgivningen.

Databehandleravtaler (Kriterie 13)

Den behandlingsansvarlige må inngå avtaler med databehandlere som skal behandle personopplysninger på vegne av den behandlingsansvarlige, heretter kalt databehandleravtale. Disse avtalene skal fastsette rammene for behandlingen, og det skal særlig angis at databehandleren: [88]

a) behandler personopplysningene bare på dokumenterte instrukser fra den behandlingsansvarlige, herunder med hensyn til overføring av personopplysninger til en tredjestat eller en internasjonal organisasjon, med mindre det kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt; i så fall skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav før behandlingen, men mindre denne rett av hensyn til viktige allmenne interesser forbyr en slik underretning,
b) sikrer at personer som er autorisert til å behandle personopplysningene, har forpliktet seg til å behandle opplysningene konfidensielt eller er underlagt en egnet lovfestet taushetsplikt,
c) treffer alle tiltak som er nødvendig i henhold til artikkel 32 (teknisk og organisatorisk sikkerhet),
d) overholder vilkårene når det gjelder å engasjere en annen databehandler,
e) idet det tas hensyn til behandlingens art og i den grad det er mulig, bistår, ved hjelp av egnede tekniske og organisatoriske tiltak, den behandlingsansvarlige med å oppfylle vedkommendes plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter,
f) bistår den behandlingsansvarlige med å sikre overholdelse av forpliktelsene med hensyn til sikkerhet og risikovurderinger, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for databehandleren,
g) etter den behandlingsansvarliges valg, sletter eller tilbakeleverer alle personopplysninger til den behandlingsansvarlige etter at tjenestene knyttet til behandlingen er levert, og sletter eksisterende kopier, med mindre unionsretten eller medlemsstatenes nasjonale rett krever at personopplysningene lagres,
h) gjør tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i denne artikkel er oppfylt, samt muliggjør og bidrar til revisjoner, herunder inspeksjoner, som gjennomføres av den behandlingsansvarlige eller en annen revisor på fullmakt fra den behandlingsansvarlige.

Databehandleren skal ikke engasjere en annen databehandler uten at det er innhentet særlig eller generell skriftlig tillatelse fra den behandlingsansvarlige, i tillegg skal den behandlingsansvarlige underrettes om eventuelle planer om å benytte andre databehandlere slik at den behandlingsansvarlige har mulighet til å motsette seg dette. Videre skal det i slike tilfeller foreligge en databehandleravtale mellom databehandleren og underleverandøren. [89]

[88] Personopplysningsloven, personvernforordningen. *Artikkel 28. Databehandler, pkt. 3*.
[89] Datatilsynet - Databehandleravtale

Punktene over er lovkravene til hva en databehandleravtale i det minste skal inneholde, det er ikke noe i veien for at den behandlingsansvarlige setter flere vilkår som går utover lovkravene. Datatilsynet anbefaler at databehandleravtalen, i tillegg til lovkravene, inneholder følgende: [90]

- Bestemmelser om vederlag og dekning av kostnader.
- Krav om at kun autoriserte personer har tilgang til opplysningene, og at tilgangen blir fjernet dersom autorisasjonen utløper eller av andre grunner ikke lenger gjelder.
- Krav om at kun autoriserte personer som av nødvendige grunner har tilgang til personopplysningene.
- Krav om at databehandleren har truffet nødvendige tiltak for å oppfylle sikkerhetsbestemmelsene etter personopplysningsloven artikkel 32. Samt at eventuelle minimumskrav til sikkerhetstiltak beskrives i et eget vedlegg til databehandleravtalen.
    - Eksempler: beskrivelser av tekniske og organisatoriske tiltak, eventuelle krav til pseudonymisering eller kryptering, eventuelle krav til logging, eventuelle krav til sikring av personopplysningene der disse lagres.
- Dersom databehandleren bruker andre databehandlere (underleverandør), en presisering av at databehandleren har det fulle ansvaret overfor den behandlingsansvarlige dersom underleverandøren ikke oppfyller sine forpliktelser etter GDPR.
- Dersom den behandlingsansvarlige skal foreta en DPIA og eventuelt forhåndsdrøftinger med Datatilsynet, bør databehandleravtalen inneholde informasjon om hva den behandlingsansvarlige forventer av databehandleren.
    - Eksempel: Krav om at databehandleren bidrar til å vurdere sikkerhetstiltak som kan bidra til å håndtere risikoen behandlingen medfører for de registrerte.
- Krav til hvordan sletting av personopplysninger spesifikt skal skje.
- En prosedyre for den behandlingsansvarliges tilsyn med databehandleren i et eget vedlegg.
- Konkretisering av hvor ofte databehandleren skal informere den behandlingsansvarlige, eller hvor ofte det skal utføres tilsyn.

Vi legger til grunn at det foreligger databehandleravtaler mellom kommunen og virksomheter som behandler personopplysninger på vegne av kommunen, og at disse i det minste oppfyller de krav som er fastsatt i personvernlovgivningen. Videre at det også foreligger databehandleravtaler mellom virksomheten som behandler personopplysninger på vegne av kommunen og eventuelle underleverandører dersom det er relevant. I tillegg legger vi til grunn at databehandleravtalene bør samsvare med anbefalingene til Datatilsynet.

Informasjonssikkerhet og personvern (Kriterie 14)

Etter personopplysningsloven skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som er egnet med hensyn til risikoene forbundet med behandlingen av personopplysninger. [91] I denne sammenhengen er det kun organisatoriske tiltak som er relevante, og som blir omtalt her.

Etterlevelse av personvernregelverket må ses i sammenheng med informasjonssikkerhetssystemet som virksomheten bruker. Organisatoriske tiltak knyttet til informasjonssikkerheten kan eksempelvis være:

- Risikovurderinger ved innføring av nye systemer, endringer i eksisterende løsninger, eller endringer i trusselbildet.

[90] Datatilsynet - Databehandleravtale
[91] Personopplysningsloven, personvernforordningen. *Artikkel 32. Sikkerhet ved behandlingen*.

- Rutiner for håndtering av dokumenter med sensitivt innhold, samt prosedyre ved tap av dokumenter med sensitiv informasjon.
- Rutiner/prosedyrer knyttet til tilgang til, lagring av, og sletting av dokumenter med sensitive personopplysninger.
- Rutiner for opplæring i bruk av virksomhetens digitale systemer.
- Rutiner for håndtering av brudd på informasjonssikkerheten.

Vi legger til grunn av kommunen har etablerte organisatoriske tiltak som sikrer et egnet informasjonssikkerhetsnivå som ivaretar vernet av personopplysninger i henhold til personvernlovgivningen. Dette innebærer blant annet at kommunen gjennomfører risikovurderinger av informasjonssikkerhetshendelser knyttet til behandling av personopplysninger.

Punktvis oppsummering av revisjonskriterier for problemstilling 2

Utledningen av krav og forventninger til kommunens arbeid med å sikre et tilfredsstillende personvern kan oppsummeres i følgende punkter:

9. Kommunen må ha et personvernombud etter regelverket, og sørge for at personvernombudet er kjent for de ansatte og andre.
10. Kommunen må ha nødvendige rutiner, prosedyrer, og praksis som sikrer tilfredsstillende håndtering av personopplysninger, og som oppdateres ved behov.
11. Kommunen må føre protokoller over alle behandlingsaktiviteter.
12. Kommunen må gi informasjon om hvordan de behandler personopplysninger, gjennom en personvernerklæring.
13. Kommunen må sørge for at det foreligger databehandleravtaler med og mellom virksomheter som behandler personopplysninger på vegne av kommunen, og disse må være i henhold til personvernlovgivningen.
14. Kommunen må gjennomføre tiltak som sørger at informasjonssikkerheten ivaretar vernet av personopplysninger i henhold til personvernlovgivningen, herunder:
    - Sørge for tilstrekkelig kompetanse i organisasjonen.
    - Gjennomføre risikovurderinger av informasjonssikkerhetshendelser knyttet til behandling av personopplysninger.

Referanser

Kommuneloven

Personopplysningsloven med lovkommentarer

eForvaltningsforskriften

Datatilsynet.no

Personvernforordningen (GDPR)

KS 2020. Orden i eget hus: Kommunedirektørens internkontroll

KS 2022. Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

Vedlegg B: Spørreundersøkelse - Data og analyse

Spørreundersøkelsen som ble sendt til ansatte med minst 50 % stilling i Stange kommune var basert på Digitaliseringsdirektoratets veileder for kartlegging av digital sikkerhetskultur i virksomheter. [92]

Undersøkelsen består av fem hovedtemaer med tilhørende spørsmål:

- Holdninger til digitalisering og digital sikkerhet
- Risiko-oppfattelse
- Synet på styring og kontroll
- Sikkerhetsatferd
- Kunnskap, læring, og interesse

Vi har gjort analyser av dataene hvor vi både har sett på hva svarene sier generelt om den digitale sikkerhetsatferden til de ansatte i kommunen, samt har vi sammenlignet ulike grupper ansatte.

Svaralternativene i mange av spørsmålene er gitt på en skala fra 1-5, hvor 1-2 er negative svar, 3 er «vet ikke», og 4-5 er positive svar. Vi har valgt å behandle 1 og 2 (negativt svar), samt 4 og 5 (positivt svar), som felleskategorier i analysen av svarene. Dersom man har svart 3 på skalaen, har man i utgangspunktet ikke tatt stilling til spørsmålet. Det er med andre ord nyanser i tallmaterialet som vi har valgt å se bort ifra for å forenkle analysen av svarene.

Generelle innledende betraktninger

De aller fleste ansatte mener de er i stand til å vurdere hva som er trygt eller utrygt å gjøre på internett, men dette samsvarer ikke helt med svarene på hvorvidt man forbinder spesifikke aktiviteter med høy risiko.

En betydelig andel av ansatte uten lederansvar oppga at de ikke vet om virksomheten har regler for digital sikkerhet (21 %). I tillegg svarte 26 % av ansatte uten lederansvar at de enten ikke har fått, eller vet om de har fått, opplæring i digital sikkerhet.

Holdninger til digitalisering og digital sikkerhet

Flertallet av de ansatte svarte at de opplever ledelsen som gode rollemodeller når det gjelder digital sikkerhet (62 %), mens cirka en femtedel (24 %) svarte «Vet ikke» på dette spørsmålet.

Mange ansatte svarte at det er lav terskel for å si ifra til kollegaer dersom de ser at en kollega gjør noe som utgjør en digital risiko for virksomheten (79 %), mens kun en femtedel (21 %) opplever at kollegaer sier ifra i slike tilfeller. Undersøkelsen er i seg selv ikke stand til å gi informasjon om slike digitale sikkerhetshendelser forekommer.

Risiko-oppfattelse

På spørsmål om man er i stand til å vurdere hva som er trygt eller utrygt å gjøre på internett, svarte de aller fleste (92 %) at de i stor grad er i stand til å vurdere dette på egenhånd.

Videre i undersøkelsen ble de ansatte spurt om de var bekymret for:

- Å bli hetset eller mobbet på internett på grunn av stillingen sin
- Å få datavirus på arbeidsgivers datautstyr

[92] Digdir.no – Veileder for kartlegging av digital sikkerhetskultur

- Å bli lurt til å gi fra seg informasjon
- At virksomheten skal bli utsatt for målrettede digitale angrep fra eksterne aktører
- At virksomheten skal bli utsatt for digitale angrep fra utro tjenere
- At virksomheten skal bli utsatt for svikt i digitale systemer som følge av utilsiktede feil
- At man mister arbeidsgivers data

Resultatene fra undersøkelsen viser at flertallet av de spurte i liten grad er bekymret for at digitale trusler/hendelser skal skje dem. Det er mest bekymring knyttet til at arbeidsplassen skal bli utsatt for svikt i digitale systemer på grunn av utilsiktede feil eller at man skal bli utsatt for målrettede angrep fra eksterne aktører, men også ved disse faktorene var det kun et fåtall som svarte at de er bekymret for at det skal skje dem.

I undersøkelsen ble de ansatte også spurt hvorvidt de forbinder følgende aktiviteter med høy risiko:

- Bruk av epost
- Deling av jobb-passord med andre
- Bruk av sosiale medier
- Bruk av digitale assistenter
- Bruk av minnepinner og liknende
- Bruk av sky-tjenester
- Mottak av SMS-er med lenker

Resultatene viser at de ansatte generelt sett forbinder alle aktivitetene beskrevet over med risiko, men resultatene knyttet til to aktiviteter skiller seg fra våre forventninger. Vi hadde forventet at en enda høyere andel av de ansatte skulle svare at de forbinder bruk av epost og mottak av SMS-er med lenker med høy risiko.

Over halvparten av de ansatte svarte at de i liten grad forbinder bruk av epost med høy risiko (68 %). Innholdet i eposter er ikke sikret på noen måte, så det er overraskende at så mange ansatte mener risikoen er liten. Videre står dette i kontrast til at de aller fleste ansatte tidligere i undersøkelsen oppga at de var i stand til å vurdere hva som er trygt eller utrygt å gjøre på internett.

Flesteparten svarte at de forbinder å dele jobb-passord med andre som høy risiko (82 %), men det er likevel en tankevekker at nesten en femtedel (18 %) enten ikke forbinder dette med høy risiko eller ikke vet om de forbinder dette med høy risiko. Å dele passord med andre øker sjansen for at passordet havner på avveie, og konsekvensene ved at uvedkommende får tak i ditt passord og tilgang til kommunens lukkede systemer kan være svært alvorlige.

Også når det gjelder mottak av SMS-er med lenker, svarte flesteparten at de forbinder dette med høy risiko (74 %). Likevel mener vi det er bekymringsfullt at cirka en fjerdedel (26 %) ikke forbinder dette med høy risiko, eller ikke vet at dette er forbundet med høy risiko. SMS-svindel er en av de mest utbredte metodene som brukes for å stjele informasjon, og det kan være krevende å vurdere om SMS-en kommer fra en sikker eller usikker aktør. Spørsmålet tar ikke stilling til den spurte sin evne til å vurdere hvorvidt er SMS med lenke er ekte eller falsk, men å motta SMS-er med lenker er uansett alltid forbundet med høy risiko.

Synet på styring og kontroll

I undersøkelsen ble de ansatte spurt om de kjente til virksomhetens regler for digital sikkerhet, om disse reglene er til hinder for deres daglige gjøremål på jobb, og hvorvidt man iblant bevisst bryter

reglene. Flertallet svarte at de var kjent med virksomhetens regler for digital sikkerhet (81 %), de fleste mener ikke at reglene er til hinder for daglige gjøremål (91 %), og det var kun et fåtall (3 %) som svarte at det hender de bryter reglene for digital sikkerhet bevisst.

En betydelig andel av de ansatte svarte at de ikke vet om virksomheten har regler for digital sikkerhet, og dersom man bruker en krysstabulering [93] med hensyn til lederansvar blir dette enda tydeligere. En femtedel (21 %) av ansatte uten lederansvar, oppga at de ikke vet om virksomheten har regler for digital sikkerhet. Dersom man bruker en krysstabulering med hensyn til ansiennitet ser man at det er de ansatte med lengst ansiennitet (over 10 år) som i størst grad er usikre på om virksomheten har regler for digital sikkerhet (20 % svarte «vet ikke»). Samtidig er ansatte med kortest ansiennitet (under 1 år) i størst grad sikre på samme spørsmål (14 % svarte «vet ikke»).

Videre ble det stilt spørsmål om den ansatte er klar over hvem det skal meldes fra til om digitale sikkerhetshendelser. For dette spørsmålet ble de som svarte bekreftende ledet til et oppfølgingsspørsmål, hvor de ble bedt om å skrive i et åpent tekstfelt hvem de skal melde fra til. Det var 439 personer (82 %) som svarte at de vet hvem de skal melde fra til om digitale sikkerhetshendelser, men det var kun 381 personer (71 %) som svarte på oppfølgingsspørsmålet. Av svarene på oppfølgingsspørsmålet oppga de aller fleste at skal melde fra til nærmeste leder og Indigo IKT, samt IKT-ansvarlig/sikkerhetsansvarlig i Stange kommune. Enkelte svarte også at de ville rapportere hendelsen til Datatilsynet eller registrere den i kommunens avvikssystem.

På spørsmål om man opplever at ledelsen har kommunisert tydelig hvilke forventninger de har til den enkelte ansatte når det gjelder digital sikkerhet, var svarene ganske delt. Litt over halvparten (59 %) opplever at dette er kommunisert tydelig, mens cirka en tredjedel (35 %) opplever at dette ikke er tydelig kommunisert, og en liten andel svarte at de er usikre på dette.

Sikkerhetsatferd

På spørsmål om de ansatte undersøker om nettsider og eposter er sikre, oppgir de aller fleste at de gjør slike vurderinger. Kun 4 % oppga at de ikke kontrollerer nettsider før de bruker dem, og kun 5 % oppga at de ikke kontrollerer lenker og vedlegg mottatt på epost før de åpner dem.

Flertallet oppga at de ikke bruker de samme passordene i flere av systemene de bruker i jobbsammenheng (62 %), og de aller fleste svarte at de ikke bruker de samme passordene hjemme som på jobb (90 %). En fare ved å bruke samme passord på jobb som man bruker hjemme, er at det utgjør en risiko for arbeidsplassen dersom man mister kontrollen over et passord i privat sammenheng. Det er også viktig at man ikke gjenbruker passord i flere systemer på jobb, slik at man hindrer at flere systemer blir kompromittert samtidig dersom et passord skulle havne på avveie.

Det er kun 7 % som svarte at de ikke låser skjermen når de forlater datamaskinene sin på jobb. Videre oppga 98 % at de ikke poster informasjon om jobben sin på sosiale medier som privatperson.

De ansatte ble også spurt om hva de gjør om de opplever følgende:

- Mottar en mistenkelig epost
- Mistenker at man har datavirus på kommunens datamaskin

[93] Krysstabulering vil si å sammenligne resultater fra forskjellige variabler. Man kan dermed sammenligne svarene på spesifikke spørsmål fra ulike respondentgrupper, som for eksempel å kun se svarene fra respondenter som har svart at de har lederansvar eller ikke.

- Ser at en kollega begår et sikkerhetsbrudd

Uavhengig av tilfelle vil de fleste varsle til sin nærmeste leder, Indigo support, eller lignende. Ved mistanke om virus på kommunens datamaskin oppga 93 % at de ville ha kontakt nærmeste leder og/eller Indigo support. Ved mottak av en mistenkelig epost svarte 19 % at de enten ville ha ordnet opp selv eller be en kollega om hjelp, mens 75 % ville ha varslet nærmeste leder og/eller Indigo support. Dersom man hadde observert at en kollega begår et sikkerhetsbrudd svarte 29 % at de enten ville ordnet opp selv eller bedt en kollega om hjelp, mens 57 % ville ha varslet nærmeste leder og/eller Indigo support, og 14 % svarte at de ikke vet hvordan de skal håndtere en slik hendelse.

Kunnskap, læring, og interesse

Flertallet av de ansatte svarte at de hadde fått opplæring i digital sikkerhet (77 %), men vi mener at andelen burde har vært høyere. Dersom man gjør en krysstabulering for lederansvar og det enkelte virksomhetsområde ser man noen interessante forskjeller. Med hensyn til lederansvar svarte 89 % av ansatte med lederansvar at de har fått opplæring, mens andelen ansatte uten lederansvar som har fått opplæring er 74 %. Når det gjelder opplæring i digital sikkerhet innenfor de ulike virksomhetsområdene er det fire områder som skiller seg ut ved at under 75 % svarte at de har fått opplæring:

- Tilrettelagte tjenester (53 %)
- Barnehage (60 %)
- Ungdomsskole (71 %)
- Helsetjenester i hjemmet (74 %)

I de øvrige virksomhetsområdene oppga 75-100 % at de hadde fått opplæring i digital sikkerhet.

På spørsmål om hvordan den ansatte vanligvis lærer om digital sikkerhet, svarte flertallet (77 %) at dette vanligvis skjer gjennom interne kurs eller utdanning, eller gjennom andre tiltak satt i gang av arbeidsgiver. Resultatene tyder på at kommunen er den viktigste pådriveren til å øke de ansattes kompetanse om digital sikkerhet.

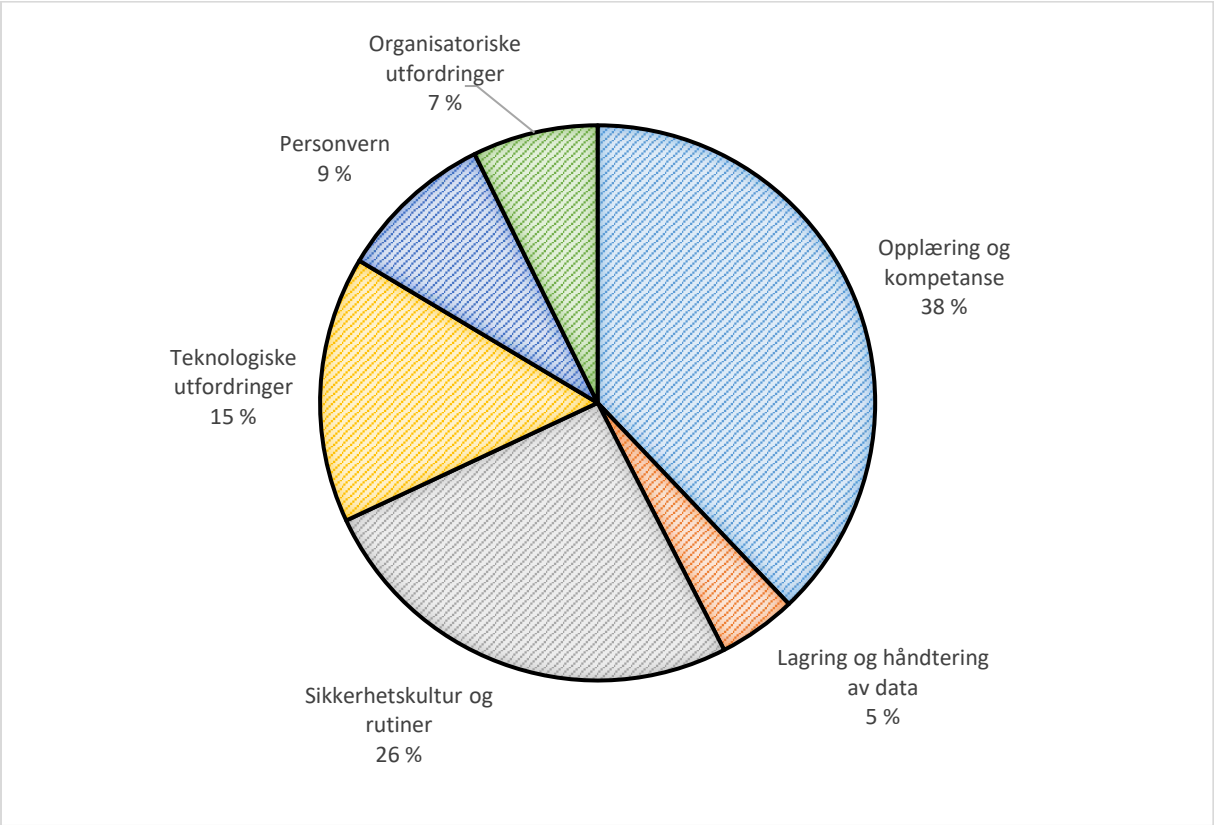
På spørsmål om man ønsket mer kunnskap om digital sikkerhet på jobb, svarte halvparten (50 %) positivt på dette, mens en fjerdedel svarte negativt (25 %) og den siste fjerdedelen svarte vet ikke (26 %). Undersøkelsen inkluderte også et spørsmål om hvilke temaer innen digital sikkerhet man ønsket mer kunnskap om, og det var mulig å velge flere alternativer. Det var totalt 462 svar på dette spørsmålet, noe som utgjør 86 % av de som svarte på spørsmål om de ønsket mer kunnskap om digital sikkerhet. Responsen tyder på at en betydelig andel flere ansatte er interessert å lære mer om digital sikkerhet enn hva som fremkom av det foregående spørsmålet, og er et tydelig signal om at de aller fleste ansatte ønsker mer kunnskap om digital sikkerhet. Temaene flest svarte at de ønsker mer kunnskap om er digitale trusler, sky-tjenester, og varsling av sikkerhetshendelser i egen virksomhet. Den fulle listen med svarprosent er som følger:

- Sikker bruk av epost (33 %)
- Hvordan behandle arbeidsrelatert informasjon (33 %)
- Sikker bruk av sosiale medier (22 %)
- Hvordan lage sikre passord (16 %)
- Sikker bruk av mobile enheter (33 %)
- Sikkerhet på reise (15 %)
- Varsling av sikkerhetshendelser i egen virksomhet (41 %)
- Digital trusler (60 %)

- Sky-tjenester (47 %)

Hovedutfordring for digital sikkerhet

Avslutningsvis i undersøkelsen inkluderte vi et åpent spørsmål [94] om hva de ansatte mener er den største utfordringen for den digitale sikkerheten i deres virksomhet. Vi mottok totalt 270 svar på dette spørsmålet, hvorav 219 av svarene var konstruktive. [95] Vi har gjennomgått svarene og forsøkt å kategorisere disse for å finne ut hva de ansatte mener er mest utfordrende, og hva de selv mener det bør jobbes mer med i kommunen. Vi sorterte svarene innenfor seks ulike temaer:



Av svarene ser vi at den største andelen av de som besvarte spørsmålet mener at opplæring og kompetanse er hovedutfordringen til kommunen når det gjelder digital sikkerhet (38 %). Dernest omhandler en betydelig andel av svarene enten sikkerhetskultur og rutiner (26 %) eller teknologiske utfordringer (15 %). De øvrige svarene er knyttet til enten personvern, organisatoriske utfordringer, eller lagring og håndtering av data.

Oppsummering

De tydeligste funnene i undersøkelsen er:

- Flertallet av de ansatte opplever ledelsen som gode rollemodeller når det gjelder digital sikkerhet.
- Det er lav terskel for å si ifra til kollegaer dersom de gjør noe som utgjør en digital risiko, men et fåtall har opplevd at kollegaer sier ifra i slike tilfeller.

[94] Spørsmålet ble stilt i form av et åpent tekstfelt hvor respondenten selv skrev sin mening.
[95] Svar som for eksempel «Vet ikke» og «Usikker» ble fjernet.

- Forholdet mellom ansatte som mener de er i stand til å vurdere hva som er trygt og utrygt å gjøre på nett, og den risikoen de anser ved handlinger på nett - spesielt med hensyn til bruk av epost og mottak av SMS-er med lenke - tyder på at en betydelig andel ansatte overvurderer sin egen kunnskap om digital sikkerhet.
- Flesteparten av de ansatte er kjent med virksomhetens regler for digital sikkerhet, og følger disse. Likevel er det en betydelig andel av de ansatte uten lederansvar som ikke er klar over virksomhetens regler for digital sikkerhet.
- Et flertall av de ansatte svarte at de vet hvem de skal melde fra til ved en digital sikkerhetshendelse, men ikke alle disse var i stand til å bekrefte dette i et oppfølgingsspørsmål.
- Et flertall oppga at de ikke gjenbruker passord i jobb-sammenheng, og de aller fleste bruker ikke samme passord på jobb som de bruker privat.
- Flesteparten av de ansatte har fått opplæring i digital sikkerhet, men det er en forskjell på ansatte med og uten lederansvar, samt innenfor enkelte av virksomhetsområdene.