Revisjon Øst IKS

FORVALTNINGSREVISJONSRAPPORT

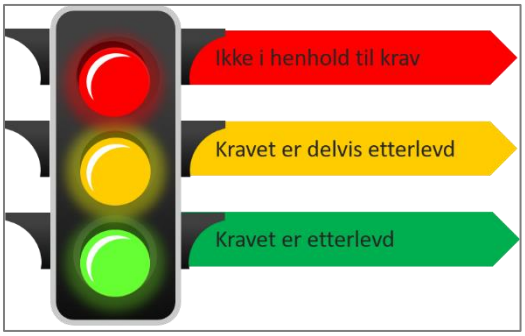
# INFORMASJONSSIKKERHET

HAMAR KOMMUNE 2022

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 pedagogisk 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, gul/oransje og rødt.

Vi gjør oppmerksom på at vurderinger med gul/oransje og rødt vil følge av beskrivelser av de mangler og/eller forbedringsmomenter vi mener at tjenesten har. For leseren vil det derfor være nyttig å lese gjennom vurderingene som fremgår av underkapitlene for hver problemstilling, i tillegg til den informasjonen leseren får i sammendraget.

Rapporten er for øvrig 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 (kap. 1),
- problemstillingen (kap. 7),
- valg av metoder og vurdering av datagrunnlag (kap. 4),
- revisjonskriterier (vedlegg A),
- presentasjon av data (kap. 7),
- vurderinger (kap. 7),
- konklusjon (kap. 8),
- anbefalinger (kap. 9),
- referanser (kap. 11) og
- kommunedirektørens uttalelse (kap. 10).

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.

Løten, den 25. august 2022

Jo Erik Skjeggestad
Oppdragsansvarlig forvaltningsrevisor

Magnus Michaelsen
Utøvende forvaltningsrevisor

# Innholdsfortegnelse

# Sammendrag

Denne rapporten er resultatet av en forvaltningsrevisjon gjennomført vinteren og våren 2021/2022. Prosjektet har hatt som problemstilling å undersøke i hvilken grad Hamar kommune har etablert en god sikkerhetskultur i organisasjonen.

Fokuset på kontrollen har i stor grad ligget til kommunens overordnede styrings- og internkontrollsystem. Dette skyldes at vi i sikkerhetskultur har lagt en forventning om at man må ha overordnede føringer for at det skal etableres en god praksis.

Datainnsamlingen i prosjektet har foregått i perioden februar 2022 - juni 2022. Vi har gjennomført en omfattende spørreundersøkelse rettet mot kommunens ansatte med minimum 50 % stilling og e-postadresse innenfor Hamar kommunes domene. Undersøkelsen ble sendt til 2477 ansatte og vi mottok svar fra 29 %. Ut ifra utvalget anses undersøkelsen derfor som representativ.

Vi har på bakgrunn av spørreundersøkelsen gjort et utvalg blant systemansvarlige for de større fagsystemene i kommunen. Dette gjelder fagsystemer med potensielt mange personopplysninger: Gerica (pasientjournalsystem), Socio (Nav), ESA (sak- og arkivsystem) og Visma Flyt Skole (opplæring og oppvekst). Det er gjennomført et oppstartsmøte, fem intervjuer, en telefonsamtale og løpende dialog på e-post med kommunens kontaktperson i prosjektet samt med arkiv knyttet til arkivert dokumentasjon. Totalt har vi hatt kontakt med ni personer i prosjektet.

I prosjektet har vi funnet at Hamar kommune har et forbedringspotensial knyttet til:

- Risikovurderinger for informasjonssikkerhet
- Rutiner for DPIA (vurderinger av personvernkonsekvenser for systemer og behandlinger)
- Rutiner for endring og avslutning av tilganger, og gjennomgang av autorisasjoner
- Identifisering av personopplysninger, formålet for behandling og oversikt over hva og hvordan opplysninger blir behandlet
- Oversikt over databehandleravtaler
- Opplæringstiltak

Vi har funnet at Hamar kommune ikke har:

- Utarbeidet retningslinjer for privat bruk av informasjonssystemer og utstyr
- Utarbeidet nødvendige rutiner og prosedyrer for håndtering av personopplysninger
- Sørget for at rutinene og prosedyrene blir oppdatert til interne frister
- Utarbeidet tilfredsstillende personvernerklæring
- Sikret at kommunens system for informasjonssikkerhet og personvern tilfredsstiller en anerkjent standard iht. eForvaltningsforskriften § 15.

Vi har imidlertid funnet at kommunen har en tilfredsstillende informasjonssikkerhetsstrategi, et tilfredsstillende avvikssystem og at man har et personvernombud.

**Samlet sett mener vi at Hamar kommune har et forbedringspotensial med hensyn til å etablere en sikkerhetskultur, noe vi mener starter med selve styringssystemet, herunder risikobasert internkontroll.**

Informasjon vi har mottatt i intervjuer tyder imidlertid på at det er mange prosesser i gang. Rett & Rimelig-prosjektet består av flere momenter som skal lede frem til at de samarbeidende kommunene for eksempel får på plass en tilfredsstillende GDPR-løsning i begynnelsen av 2023, og at man får utarbeidet rutiner ut ifra de behovene som er kartlagt i prosjektet.

Vi har også fått informasjon i intervjuer knyttet til begrensninger i fagsystemer som øker risiko for feil, men som er identifisert og som man arbeider med å lukke. Dette gjelder for eksempel Visma Flyt Skole hvor informasjon knyttet til særskilte vedtak ligger i en gradert mappe i ESA, slik at ledelsen ved skolene må skrive ut informasjonen på papir når lærere har behov for den.

Et annet eksempel er ESA, som er i ferd med å bli faset ut av leverandør og hvor kommunen nå får begrenset brukerstøtte. På skole skal det fases inn et supplerende system som skal bidra til at nåværende praksis opphører, mens det er i gang en prosess for å finne en erstatningsløsning til ESA.

Et tredje eksempel er tilfeller hvor det blir tatt bilder av sår og brukere/pasienter i helse- og omsorgstjenesten for å sikre at andre regelverk etterleves med hensyn til dokumentasjon og medisinhåndtering. Slike bilder blir ikke arkivert på tilfredsstillende måte fordi fagsystemet ikke har tillatt lagring av bilder. Vi har fått informasjon om at en modul i Gerica-systemet som sikrer arkivering av bilder knyttet til pasientjournal vil bli faset inn.

Bruk av private mobiltelefoner både i forbindelse med skole-hjem-kontakt og i helse og omsorg, introduserer en risiko for at personopplysninger ligger lagret på private medier. Kommunen har et ansvar for at slike opplysninger blir slettet ved opphør av arbeidsforhold.

Basert på våre funn har vi følgende anbefalinger til Hamar kommune:

- Kommunen må sikre et tilfredsstillende system for informasjonssikkerhet og personvern. Dette innebærer:
    - Systematiske og dokumenterte risikovurderinger for informasjonssikkerhet
    - Dokumenterte vurderinger for akseptabel risiko
    - Utarbeide nødvendige rutiner for informasjonssikkerhet og personvern, og holde disse oppdatert, inkludert rutine for DPIA som forsikrer forankring i ledelsen
    - Utarbeide opplæringsplan mht. informasjonssikkerhet og personvern
    - Planlegge og gjennomføre sikkerhetsrevisjoner
    - Ta stikkprøver innenfor informasjonssikkerhet og personvern i forbindelse med internkontrollen
- Kommunen bør sørge for at det blir foretatt jevnlig gjennomgang av og kontroll med tilganger i fagsystemene.
- Kommunen må sikre at personopplysninger blir slettet fra private medier ved opphør av arbeidsforhold, når arbeidsforholdet forutsetter bruk av privat medium, som for eksempel mobiltelefon.
- Kommunen må utarbeide en tilfredsstillende personvernerklæring som gjøres kjent for kommunens ansatte og innbyggere.
- Kommunen bør gjøre rutinene kjent i organisasjonen.

# 1 Bakgrunn for prosjektet

I henhold til kommuneloven § 23-2, punkt c, skal kontrollutvalget 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 (§ 23-3, første ledd).

Kontrollutvalget i Hamar kommune la til informasjonssikkerhet som del av sin plan for forvaltningsrevisjon og eierskapskontroll 2020-2023, vedtatt av kommunestyret i møte 24. februar 2021 (sak 12/21). Kontrollutvalget igangsatte undersøkelser av temaet gjennom orienteringer fra Hedmark IKT og kommunedirektøren, først i møte 9. mars 2021 (sak 16/21), deretter den 8. juni 2021 (sak 30/21).

Den 9. mars 2021 bestilte kontrollutvalget en forundersøkelse/prosjektplan rettet mot temaet informasjonssikkerhet (sak 16/21). Forundersøkelsen ble lagt frem i møtet den 8. juni (sak 32/21). Kontrollutvalget ønsket å gå videre med planleggingen av prosjektet og ga Revisjon Øst IKS i oppdrag å legge frem en revidert prosjektplan i møte den 7. september (sak 49/21). I dette møtet fattet kontrollutvalget følgende vedtak:

1. Revisjon Øst IKS bes om å gjennomføre forvaltningsrevisjonsprosjektet i tråd med den fremlagte planen.
2. Formålet med et forvaltningsrevisjonsprosjekt om sikkerhetskultur er å se etter om Hamar kommune har sikret en god sikkerhetskultur i organisasjonen og hvordan kommunen håndterer avvik relatert til informasjonssikkerhet. Revisjonsprosjektet skal besvare følgende problemstilling:
    a. Har kommunen etablert en god sikkerhetskultur i organisasjonen, herunder internkontroll for personvern og informasjonshåndtering, og avvikshåndtering?
3. Revisjonsprosjektet gjennomføres innenfor en timeramme på 350 timer med sannsynlig levering i april/mai 2022.

Denne rapporten er resultatet av kontrollutvalgets bestilling.

# 2 Formål og aktualitet for forvaltningsrevisjonsprosjektet

Formålet med forvaltningsrevisjonsprosjektet har vært å se etter om Hamar kommune har en god sikkerhetskultur i organisasjonen og hvordan kommunen håndterer avvik relatert til informasjonssikkerhet. Vi har i etterkant av bestillingen sett at hva vi legger i sikkerhetskultur i utgangspunktet er tilsvarende informasjonssikkerhet. Vi har derfor vektlagt informasjonssikkerhet i det videre arbeidet.

Hamar kommune hadde tilsyn fra Arkivverket i 2021, hvor det ble påpekt flere svakheter knyttet til arkivløsningen. Disse svakhetene har ligget til kommunens systemer over flere år. Det ble spesielt vist til utfordringer knyttet til personopplysningers sikkerhet som følge av papirarkiver ute i enheter utenfor rådhuset, som ikke i tilstrekkelig grad var kartlagt.

Den digitale trusselen mot norske organisasjoner, både private og offentlige, har vært økende de siste årene. Direktoratet for sikkerhet og beredskap har angitt at trusselbilde er svært høyt. Dette har det også vært flere eksempler på de siste årene, blant de mest omfattende; løsepengeangrepet rettet mot Østre Toten kommune. Russlands krigføring i Ukraina, og nasjonalpolitisk støtte og interesser, har ført til at norske offentlige organer kan bli mål i «krigen» på internett. KDD og KS har sendt et felles brev til

kommunene i mars 2022, som har satt teknologisk sikkerhet i kommune-Norge enda tydeligere på agendaen.

Temaet sikkerhetskultur er i stor grad aktuelt. Ethvert system er sjelden sterkere enn sitt svakeste ledd. Det er derfor viktig at organisasjonen har gode rutiner og systemer for å håndtere informasjon.

# 3 Avgrensninger: IKT-sikkerhet, informasjonssikkerhet, kybersikkerhet og sikkerhetskultur

I dette forvaltningsrevisjonsprosjektet er det foretatt en avgrensning. Dette forvaltningsrevisjonsprosjektet handler om informasjonssikkerhet, knyttet til datateknologi. Innenfor datateknologi opereres det med ulike sikkerhetsbegreper som belyser ulike deler av risikomomenter knyttet til bruken av datateknologien.

De tre mest omtalte formene for sikkerhet er IKT-sikkerhet, informasjonssikkerhet og kybersikkerhet. I det følgende gir vi en kort innføring i de tre begrepene.

## 3.1 IKT-sikkerhet

IKT-sikkerhet omhandler verktøy og metoder knyttet til drift av IKT-systemer og –løsninger, og å beskytte teknologibaserte systemer som lagrer, prosesserer og overfører data. [1] Kort sagt handler IKT-sikkerhet om mye av det konkrete for å forhindre at uvedkommende kan komme seg inn i IKT-løsninger og på datamaskiner, uavhengig av om man er påkoblet internett.

Brudd på IKT-sikkerheten vil kunne medføre nedetid i driftsløsningene og ha konsekvenser for daglige arbeidsoppgaver og for investeringer. Følgene av brudd på IKT-sikkerheten kan omhandle elementer som ligger til informasjonssikkerheten, for eksempel at informasjon og opplysninger kommer på avveie.

## 3.2 Informasjonssikkerhet

Informasjonssikkerhet omhandler i større grad organisasjoners overordnede prosesser og rutiner for å sikre informasjon og tjenester. Heggernes viser til at informasjonssikkerhet handler om «å sikre kontinuitet i forretningsdriften og å minimere forretningsmessig skade som følge av sikkerhetshendelser». [2]

Forskjellen på IKT-sikkerhet og informasjonssikkerhet handler med andre ord om at IKT-sikkerhet går ut på å lage tekniske løsninger som forhindrer at teknologibaserte systemer tar skade av angrep, mens informasjonssikkerhet handler om beredskap og beredskapsløsninger som kan iverksettes når en uønsket sikkerhetshendelse inntreffer.

I en presentasjon gitt i kontrollutvalget i Kongsvinger kommune den 7. juni, ble følgende modell benyttet for å illustrere de tre momentene ved informasjonssikkerhet, hva de består av og hva man har behov for kontroll på innenfor disse. Dette gjelder at man må ha:

- Styrende dokumenter hvor man setter nivå for akseptabel risiko, har et IKT-reglement og informasjonssikkerhetspolicy.
- Gjennomførende dokumenter hvor det lages rutiner for og gjennomføres IKT-anskaffelser, risikoanalyser, DPIA, [3] opplæring og nød-rutiner.

[1] Heggernes, T. A. 2020, *Digital forretningsforståelse. Fra store data til små biter* (3. utgave), s. 350.

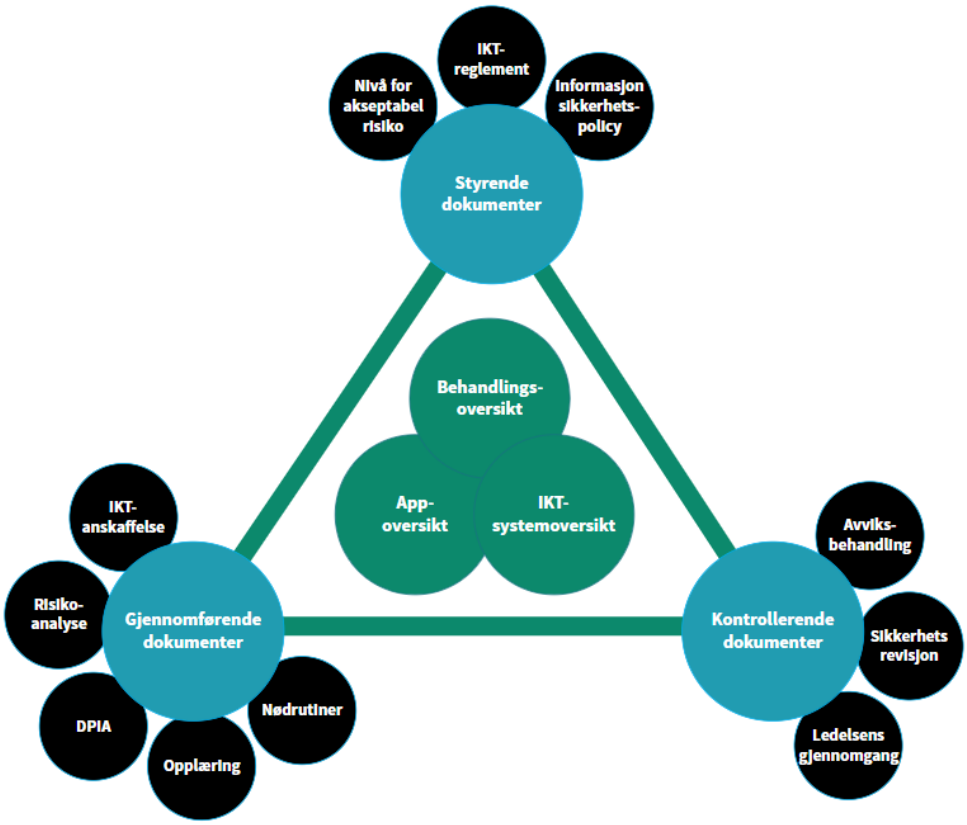
[2] Heggernes, T. A. 2020, *Digital forretningsforståelse. Fra store data til små biter* (3. utgave), s. 352.

[3] Kilde: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/

- Kontrollerende dokumenter hvor man har rutiner for og gjennomfører avviksbehandling, sikkerhetsrevisjon og hvor ledelsen foretar en gjennomgang.

Innenfor dette er det behov for en oversikt over opplysninger og informasjon som behandles, en systemoversikt over IKT-systemer, og en oversikt over brukte applikasjoner.

Informasjonssikkerhet er med andre ord i stor grad relatert til internkontrollsystem og internkontroll i praksis.




*Figur 1: Hentet fra presentasjon, kontrollutvalget Kongsvinger kommune 7. juni 2022*

## 3.3 Kybersikkerhet

Kybersikkerhet handler om å forhindre negative konsekvenser ved angrep eller uønskede hendelser som foregår over internett, men som ikke direkte berører hensyn til konfidensialitet, integritet eller tilgjengelighet på informasjon. [4] Dataenes konfidensialitet, integritet og tilgjengelighet står sentralt som verdier for både IKT-sikkerhet og informasjonssikkerhet. Som eksempler på kybersikkerhetstrusler, viser Heggernes til nettmobbing, hacking av smart-gjenstander i hjemmet, åndsverkskrenkelse ved fildeling, og kyberterrorisme. Sistnevnte kan imidlertid ha følger for konfidensialitet, integritet og tilgjengelighet.

[4] Heggernes, T. A. 2020, *Digital forretningsforståelse. Fra store data til små biter* (3. utgave), s. 353.

# 4 Metode for revisjonen

I NKRFs standard for forvaltningsrevisjon står det at man i en forvaltningsrevisjon skal bruke metoder som sikrer at de data som brukes er relevante og pålitelige, og at dataene skal være tilstrekkelige for å besvare prosjektets problemstillinger. Metodene som er brukt skal begrunnes. En måte å sikre dataenes relevans og pålitelighet på, er å innhente data om samme forhold gjennom flere metoder. For noen få problemstillinger holder det å bruke en metode, som oftest er det nok med to metoder, og det er sjelden nødvendig å bruke mer enn tre metoder. Bruk av to eller flere metoder kalles metodetriangulering.

I dette prosjektet har vi brukt metodene dokumentstudier, intervjuer og spørreundersøkelse. Vi omtaler den enkelte metode nærmere i de neste tre underkapitlene.

## 4.1 Dokumentstudier

Prosjektet har i stor grad hatt fokus på kommunens internkontroll, overordnede styringsdokumenter og rutiner, og dokumentasjon på at kommunen ivaretar kravene i personopplysningsloven og GDPR. Gjennomgang og kontroll av disse dokumentene kaller vi dokumentstudier.

Dokumentene som er brukt i dokumentstudiene blir referert til i rapporten i forbindelse med de delene av kontrollen hvor dokumentgjennomgang har vært nødvendig for å besvare prosjektets problemstilling. Dokumentene som har blitt gjennomgått har blitt oversendt oss på forespørsel. Disse dokumentenes gyldighet anses bekreftet av kommunen når de oversendes revisjonen.

## 4.2 Intervjuer

I forvaltningsrevisjonsprosjektet har vi gjennomført intervjuer med utvalgte systemansvarlige i Hamar kommune. Systemansvarlige er utvalgt basert på type system og den informasjonen som ligger i systemene. Vi valgte ut systemansvarlige for:

- Gerica, som inneholder helseopplysninger og annen sensitiv personinformasjon,
- Socio, som inneholder opplysninger knyttet til tjenestemottakere ved NAV,
- Visma Flyt Skole, som inneholder elevinformasjon, og
- ESA, som er kommunens arkivsystem og som blant annet brukes til arkivering av informasjon som kan ha sensitivt innhold.

Vi har i tillegg hatt et oppstartsmøte med assisterende kommunedirektør og leder av IKT og utvikling, samt samtaler og kontakt med leder av IKT og utvikling underveis, i forbindelse med at hun har vært vår kontaktperson i prosjektet.

Det er totalt gjennomført fem intervjuer, med til sammen seks personer, samt oppstartsmøte, løpende samtaler med kontaktperson. Det har også vært dialog med arkiv knyttet til arkiverte databehandleravtaler og med en ansatt ved innkjøpsavdelingen knyttet konkret til en databehandleravtale.

Oppstartsmøtet ble avholdt i november 2021. De øvrige intervjuene er gjennomført i perioden 19.4.22-15.6.22.

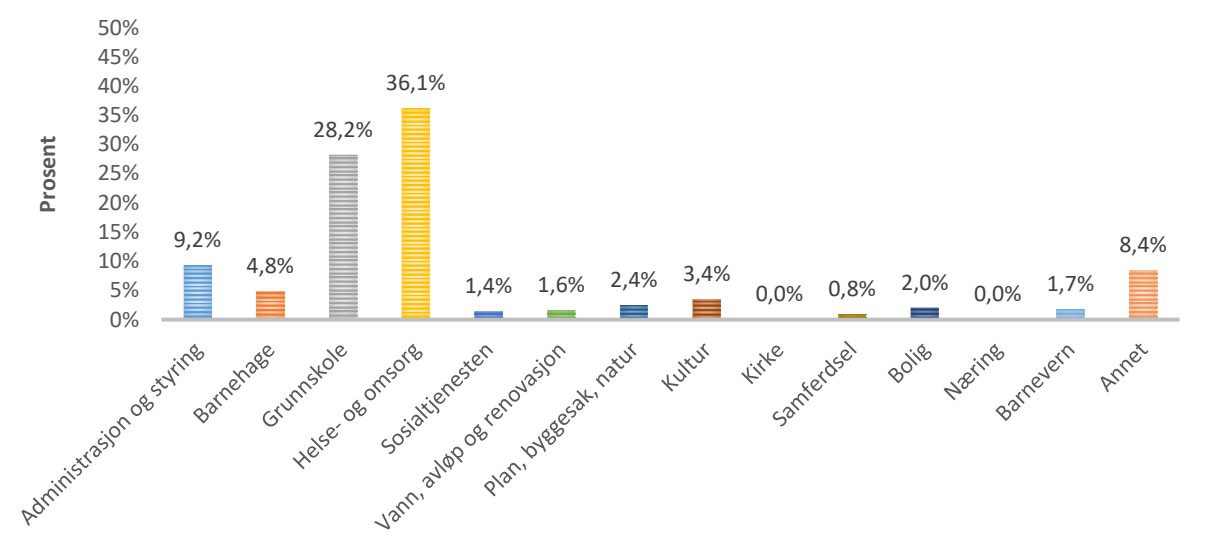
Det er utarbeidet referater fra samtlige intervjuer, og referatene er lest gjennom og godkjent av de vi har intervjuet.

## 4.3 Spørreundersøkelse

Det er gjennomført en spørreundersøkelse rettet mot ansatte i Hamar kommune med minst 50 % stillingsprosent. Spørreundersøkelsen er gjennomført i perioden 8.2.22-28.2.22. Det ble sendt

invitasjon til 2477 ansatte. Tre av invitasjonene ble avvist, det vil si at invitasjonen ikke kunne leveres. Av de leverte 2474 invitasjonene mottok vi 716 svar. Dette utgjør ca. 29 %. I tillegg hadde 279 åpnet undersøkelsen, men ikke sluttført sine svar og sendt de inn. Dette er ytterligere 11 %.

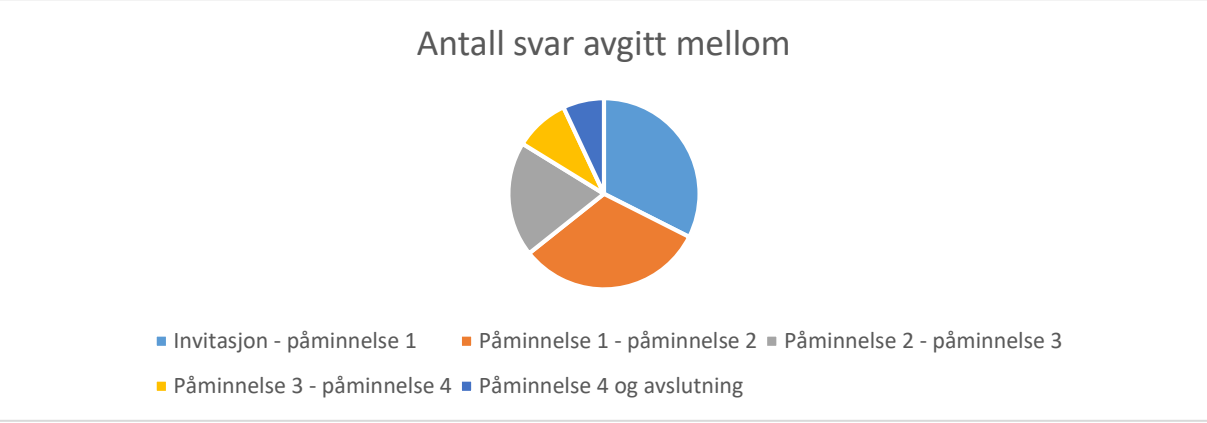
Svarene fordelte seg på følgende virksomhetsområder:




I kategorien «annet» finner man blant annet ansatte i PP-tjenesten, interkommunalt krisesenter, voksenopplæring, helsestasjon, byggteknisk drift og eiendomsforvaltning. 20 % av de som har svart har også oppgitt at de har lederansvar. Et stort flertall av besvarelsene (62 %) er gitt av ansatte som har jobbet i kommunen i 6 år eller mer – de aller fleste over 10 år (45 %).

Vi har forsøkt å få en så høy svarprosent som mulig ved blant annet å forankre undersøkelsen i kommunens ledergruppe og ved dialog med kommunens IKT-leder. IKT-leder fikk lagt ut melding om undersøkelsen på kommunens intranett i undersøkelsens siste uke grunnet en del henvendelser om hvorvidt den var trygg å besvare. Vi har oppgitt vår egen kontaktinformasjon dersom det skulle være spørsmål knyttet til undersøkelsen, men har fått få henvendelser til oss.

Det ble sendt en invitasjon den 8. februar. Deretter ble det sendt påminnelse til de som ikke hadde besvart undersøkelsen etter første invitasjon den 16., 21., 24. og 28. februar. Selv om effekten av hver påminnelse har vært avtakende, har de tre siste påminnelsene likevel bidratt til ytterligere 35 % flere svar:



# 5 Spørreundersøkelsen – data og analyse

Spørreundersøkelsen som er sendt ansatte i Hamar kommune med minimum 50 % stillingsprosent og kommunal e-postadresse har vært basert på en undersøkelse NorSIS[5] har utarbeidet for vurdering av sikkerhetskulturen i virksomheter.

Undersøkelsen består av fem hovedtemaer med tilhørende spørsmål. De fem temaene omhandler:

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

Vi har gått gjennom data både med hensyn til hva som er svarene generelt ut ifra alle svar, og gjort analyser hvor vi har sammenlignet ansatte med og ansatte uten lederansvar, samt ledere og ansatte med og uten opplæring. Vi har i tillegg sett nærmere på passord-praksis.

Svaralternativene er i mange av spørsmålene gitt på en skala fra 1-5, samt med et «vet ikke»-alternativ. Selv om det finnes artsgrader har vi valgt å behandle 1 og 2 som felleskategori og 4 og 5 som felleskategori. Dersom man svarer 3, tar man i utgangspunktet ikke stilling til spørsmålet. Det samme gjelder om man svarer vet ikke. Det er med andre ord nyanser i tallmaterialet som vi har valgt å se bort ifra for enkelhets skyld.

**Generelle innledende betraktninger**

20 % av de som har besvart undersøkelsen har oppgitt at de har lederansvar. De som har jobbet lengst i kommunen har en noe større respons på at de har mottatt opplæring enn øvrige ansatte. Av de med ansiennitet under 10 år, har bare halvparten oppgitt at de har fått opplæring i digital sikkerhet.

**Holdninger til digitalisering og digital sikkerhet**

Undersøkelsen viser at de ansatte i Hamar kommune opplever at det er lav terskel for å si ifra til kolleger dersom en ser at en kollega gjør noe som utgjør en digital sikkerhetsrisiko for virksomheten. Det er likevel slik at få opplever at kolleger gir tilbakemelding på slike forhold. Undersøkelsen er i seg selv ikke i stand til å gi informasjon om slike digitale sikkerhetshendelser forekommer.

De fleste som tar stilling til spørsmålet opplever ledelsen som gode rollemodeller.

**Risiko-oppfattelse**

Vi spurte ansatte i Hamar kommune om de opplever at de er i stand til å avgjøre hva som er trygt og utrygt å gjøre på internett. Åtte av ti mener at de i stor grad er i stand til å vurdere dette på egenhånd. Rundt 5 % mener at de i liten grad vet hva som er trygt og utrygt å gjøre på nett.

I oppfølgende spørsmål knyttet til opplevd risiko, spurte vi om de ansatte var bekymret for

- Å få virus på arbeidsgivers datautstyr
- At man blir lurt til å gi fra seg informasjon
- At virksomhetens systemer blir skadelidende som følge av utilsiktede feil
- At man mister egne og/eller arbeidsgivers data

[5] Norsk senter for informasjonssikring (NorSIS)

Resultatene viser at de ansatte er mer eller mindre delt på midten med hensyn til om de tror at digitale trusler kan hende dem. Av de fire nevnte eksemplene, er det knyttet mest bekymring til å få virus på arbeidsgivers utstyr. Det er minst bekymring knyttet til å bli lurt til å gi fra seg informasjon.

Vi stilte også spørsmål om de ansatte knytter høy risiko til

- Bruk av e-post
- Dele jobb-passord med andre kolleger
- Bruke sosiale medier
- Bruke digitale assistenter, som for eksempel smart-høyttalere eller chatbots
- Bruk av minnepinner og andre fysiske lagringsmedier
- Bruk av sky-tjenester
- Mottak av SMS-er med lenker

Litt overraskende opplever en stor andel at det i liten grad er risiko knyttet til bruk av e-post. Å sende e-poster blir ofte sammenlignet med å sende postkort. Informasjonen i e-postene er på ingen måte sikret. Derfor er vi overrasket over at mange mener risikoen er liten. Dette står også i kontrast til at de aller fleste oppgir at de er i stand til å vurdere hva som er trygt og utrygt å gjøre på nett.

I motsetning, og som forventet, knytter et stort flertall høy risiko til å dele jobb-passord med andre kolleger. Det er også en stor andel som mener det er høy risiko knyttet til SMS-er med lenker.

På spørsmål om hva de ansatte mener utgjør den største digitale trusselen, oppga over halvparten at de mener angrep utenfra som har til hensikt å skade arbeidsgiver har høyest risiko for å skje. Halvparten av de som har svart mener det er høy risiko knyttet til bruk av sosiale medier. Undersøkelsen viser at det er mindre kjennskap til digitale assistenter enn til de øvrige aktivitetene som det er spurt om.

**Synet på styring og kontroll**

Vi stilte spørsmål om de ansatte kjente til virksomhetens regler for digital sikkerhet, om reglene er til hinder for daglige gjøremål, og i hvilken grad man bevisst bryter reglene. Svarene viser at en fjerdedel av de som har svart er ukjente med virksomhetens regler for digital sikkerhet. De færreste opplever at disse reglene er til hinder i det daglige og at de er til hinder i de daglige aktivitetene. Det er en forholdsvis liten andel som er av motsatt oppfatning, og andelen som mener at reglene er til hinder samt bevisst bryter de utgjør rundt 5 % av de som har besvart undersøkelsen.

Vi stilte også spørsmål ved om de ansatte kjenner til hvem de skal melde fra til dersom de skulle ha kjennskap til at det har skjedd en digital sikkerhetshendelse. Spørsmålet er gitt åpent, slik at det ikke er gitt føringer gjennom svaralternativer. Svarene viser at en av fem ikke har kunnskap om hvem man skal si ifra til. Av de som har bekreftet at dette er kjent, melder de aller fleste ifra til nærmeste leder og HIKT. Deretter kommer leder av IKT utvikling i Hamar kommune og den lokale IT-ansvarlige i virksomheten.

Noe overraskende er det forholdsvis få som har svart at de melder til personvernombudet eller Datatilsynet. Undersøkelsen er ikke utarbeidet til å avdekke hva slags digitale sikkerhetshendelser som oftest forekommer, eller hva respondentene legger i «digital sikkerhetshendelse». Men en mulig årsak til at få har nevnt personvernombudet eller Datatilsynet kan ha sammenheng med at typer saker som oppstår som oftest ikke angår personvern, men andre typer sikkerhetshendelser.

Vi stilte spørsmål ved om i hvilken grad de ansatte opplever at ledelsen har kommunisert tydelig hvilke forventninger man har til den enkeltes praktisering av digital sikkerhet. Her er de ansatte forholdsvis

delt på midten. Tre av ti mener at dette i liten grad er blitt formidlet. Fire av ti mener at forventningene har blitt tydelig kommunisert.

**Sikkerhetsatferd**

På spørsmål om de ansatte undersøker nettsider og e-poster for om hvorvidt de er sikre, oppgir de aller fleste at de gjør slike vurderinger. Rundt en av ti sier de ikke kontrollerer nettsider, og en av tjue at de ikke kontrollerer e-poster.

En av ti oppgir at de bruker de samme passordene hjemme og på jobb. Videre oppgir fire av ti at de bruker de samme passordene på tvers av systemer som brukes i jobbsammenheng. Vi har i tillegg sett på om det er overlapp mellom de som bruker samme passord privat og i jobb, og de som bruker samme passord i flere systemer. Bakgrunnen for dette er at dersom man skulle miste kontrollen over passordet i det private, vil det potensielt utgjøre en risiko for arbeidsplassen på flere områder. Av de som bruker samme passord privat og i jobbsammenheng, bruker over 60 % også samme passord på tvers av systemer i det daglige arbeidet. Her er det ingen andelsmessig forskjell på ledere og ansatte, selv om utvalget er forholdsvis lite med hensyn til til å trekke tydelige sammenligninger. Det er verdt å merke seg at av de som bruker samme passord privat og på jobb, har 40 % oppgitt at de også har fått opplæring i digital sikkerhet.

En av ti oppgir at de aldri låser skjermen når man forlater datamaskinen. Undersøkelsen viser at svært få poster informasjon om sitt arbeid i sosiale medier som privatpersoner.

De ansatte ble spurt om hva de vil gjøre dersom de:

- Mottar en mistenkelig e-post
- Mistenker at man har fått virus på virksomhetens datamaskin
- Ser at en kollega begår et sikkerhetsbrudd

Uavhengig av tilfelle vil de fleste kontakte nærmeste leder, helpdesk eller lignende. Svarene viser også at de ansatte er mye tryggere på hva de skal gjøre ved mistanke om virus, siden 94 % oppgir at de ville ha varslet nærmeste leder og/eller helpdesk. Dersom man mottar en e-post ville 15 % ha ordnet opp selv. Denne andelen øker til 19 % dersom det handler om at en kollega gjør noe galt. Det er også 15 % som ikke vet hva de skal gjøre dersom en kollega foretar et sikkerhetsbrudd.

**Kunnskap, læring og interesse**

Omtrent halvparten av de som har besvart undersøkelsen har fått opplæring i digital sikkerhet. Deltakelse i opplæring blir vanligvis gjennomført ved at arbeidsgiver informerer om kurs.

Flertallet oppgir at de ønsker mer kunnskap om digital sikkerhet, mens en fjerdedel oppgir at de ikke har behov for dette. Dette betyr at selv om et overveldende flertall mener de er i stand til å vurdere hva som er trygt og utrygt å gjøre på nett, ønsker mange også mer opplæring i digital sikkerhet. Dette kan ha sammenheng med at det digitale landskapet er i kontinuerlig endring. Men det at mange mener de er i stand til å vurdere trygg atferd på nett kan også skyldes uvitenhet. Noen av resultatene i undersøkelsen tyder nettopp på dette, for eksempel ved vurdering av hvor stor risiko det er å benytte e-post som kommunikasjonsmiddel.

Blant de som ønsker mer opplæring, oppgir disse at de ønsker mer kunnskap om digitale trusler, sikker bruk av e-post, hvordan man skal behandle arbeidsrelatert informasjon på en sikker måte, og varsling av sikkerhetshendelser i virksomheten.

**Størst utfordring?**

I undersøkelsen er det stilt et spørsmål om hva respondentene mener er den største utfordringen knyttet til informasjonssikkerhet. Spørsmålet er stilt som et åpent spørsmål og vi har fått i underkant av 300 svar. Disse er gjennomgått og vi har forsøkt å kategorisere svarene for å se hva ansatte mener er mest utfordrende med informasjonssikkerhet, og hva de mener det bør jobbes mer med.

Svarene viser at et stort flertall – nærmere halvparten av respondentene – mener at brukerfeil er den største utfordringen, og at dette kommer av mangel på kunnskap og kompetanse om hvordan man praktiserer informasjonssikkerhet i det daglige. Deretter nevner halvparten så mange at det er risiko knyttet til lagring av personopplysninger og at opplysninger kan komme på avveie. Det blir i disse tilfellene nevnt at systemene for arkivering og håndtering av personinformasjon ikke er gode nok, eller at de er for begrensende slik at det etableres praksiser som utgjør andre risikoer for personvern. Ut i fra svarene ser det ut til at det for en del av respondentene gjelder systemene i skolesektoren.

Som nummer tre på listen, rett etter personopplysninger, mener 20 % av respondentene at det er utfordringer knyttet til eksterne trusler, som hacking og virus.

**Oppsummering**

De tydeligste funnene i undersøkelsen er:

- De ansatte opplever at det i liten grad har blitt gitt opplæring i digital sikkerhet.
- Det er åpenhet for å si ifra, men få gjør dette i praksis.
- 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 e-poster – tyder på en overvurdering av egne kunnskaper om digital sikkerhet.
- 25 % er ukjente med virksomhetens regler for digital sikkerhet.
- 20 % vet ikke hvor/hvem de skal melde fra til ved digitale sikkerhetshendelser.
- 30 % opplever at ledelsen i liten grad har kommunisert forventninger til den enkeltes praktisering av digital sikkerhet.

**Øvrige betraktninger**

Vi har valgt å gjennomføre en litt dypere analyse av svarene i undersøkelsen ved å se på om det er forskjell på ledere og øvrige ansatte, og om man kan se effekter av opplæringstiltak med hensyn til risikovurderinger av digital aktivitet.

**Effekter av opplæringstiltak**

Vi har funnet at de som har fått opplæring:

- opplever i større grad at ledelsen er gode rollemodeller for digital sikkerhet.
- opplever i større grad at de er i stand til å vurdere hva som er trygt og utrygt å gjøre på nett.
- er i større grad klar over at virksomheten har regler for digital sikkerhet.
- er i større grad klar over hvem de skal melde fra til om digitale sikkerhetshendelser.
- opplever i større grad at ledelsen har kommunisert tydelig hvilke forventninger de har til digital sikkerhet hos de ansatte.
- er i større grad bekymret for virus på arbeidsgivers datamaskiner, at utilsiktet feil vil kunne skade virksomhetens systemer, og mer bekymret for tap av data.
- mener i større grad at det er knyttet risiko til bruk av e-post, deling av jobb-passord med andre ansatte, bruk av sosiale medier, bruk av fysiske lagringsmedier, og bruk av sky-tjenester.

Litt overraskende er det at det er liten forskjell på de med og de uten opplæring med hensyn til risikovurdering ved bruk av e-post. De som har fått opplæring knytter også mindre risiko til bruk av fysiske lagringsmedier enn de uten opplæring. Det vil da si at opplæringen som har blitt gitt har hatt liten effekt på opplevd risiko ved bruk av e-post og bruk av fysiske lagringsmedier.

**Ledere kontra øvrige ansatte**

Når vi kontrollerer ledere mot øvrige ansatte, finner vi at ledere:

- i større grad har fått opplæring i digital sikkerhet enn øvrige ansatte, men at tre av ti ledere likevel ikke har fått opplæring.
- har generelt sett en klarere oppfatning av at ledelsen i større grad er gode rollemodeller for digital sikkerhet, og at ledelsen har kommunisert tydelig hvilke forventninger de har til praktisering av digital sikkerhet.
- er i større grad kjent med virksomhetens regler for digital sikkerhet og hvem man skal melde fra til om digitale sikkerhetshendelser.

Det er likevel verdt å merke at en av ti ledere ikke vet om virksomheten har regler for digital sikkerhet.

**Ledere med opplæring kontra ledere uten opplæring**

Dersom vi ser på forskjeller mellom ledere med og uten opplæring, ser vi at ledere med opplæring:

- knytter større risiko til bruk av e-post og sky-tjenester enn ledere uten opplæring. Forskjellen mellom ledere med og uten opplæring er større enn den er for ansatte med og uten opplæring.
- mener det er større grad av risiko knyttet til at utilsiktede feil kan medføre skade på eller svikt i virksomhetens systemer.
- bruker i mindre grad samme passord privat og i jobb enn ledere uten opplæring.

# 6 Tallmateriale

I prosjektet har vi mottatt en årsapport for IKS-sikkerhetsarbeid og sikkerhetshendelser i 2021, som vil bli nevnt mer utfyllende nedenfor. I denne årsrapporten er det gitt noe statistikk knyttet til gjennomførte tiltak i 2021, samt til sikkerhetshendelser og lignende. Det følgende kan være av interesse som bakgrunn for Hamar kommunes arbeid med informasjonssikkerhet.

- Det ble gjennomført **8 vurderinger av personvernkonsekvenser** (Data Protection Impact Assessment – DPIA) for systemer, moduler og behandlingsaktiviteter. [6]
- HIKT gjennomførte nasjonal sikkerhetsmåned i november, og benyttet en e-læringsløsning fra NorSIS som opplæringsopplegg overfor ansatte. Kun **2 % fullførte opplegget**, og deltakerprosenten var generelt lav.
- Hamar kommune har **188 datasystemer** registrert i sin sikkerhetsoversikt, men antallet kan være høyere.
- Det er registrert **143 behandlinger** for systemene. Dette tallet skulle ha vært høyere enn antallet systemer.
- Det er **1600 Teams-grupper** i Hamar kommune.
    - **1068 av gruppene er eid av oppvekstsektoren**.
    - **954 har kun en eier**. Dersom denne eieren slutter vil ikke gruppen ha eieradministrator. Det blir derfor vist til at det bør være minst to eiere.
    - **328 av gruppene har kun en eller to medlemmer**.
- Av 4830 innmeldte avvik i 2021 omhandlet **98 brudd på personvern eller IKT-sikkerhet**.
    - **95 % er meldt av helse og omsorg**. De fleste avvikene er relatert til feilført journal, og skyldes som oftest slurv eller brudd på prosedyre eller lokal rutine. Slike avvik blir meldt inn fordi når det er lagret feil på journal, er det kun systemansvarlig som kan korrigere journalen.
- Det ble sendt **1 avvik til Datatilsynet** i 2021.

[6] En DPIA gjennomføres for å sikre at personvernet til de som er registrert i løsningen/systemet blir ivaretatt.

# 7 Problemstilling – Sikkerhetskultur, internkontroll og avvikshåndtering

**Problemstilling:**

Har kommunen etablert en god sikkerhetskultur i organisasjonen, herunder internkontroll for personvern og informasjonshåndtering, og avvikshåndtering?

## 7.1 Revisjonskriterier

Følgende er en tabell med de revisjonskriteriene vi har benyttet for å besvare problemstillingen. 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 kriteriet. Fargekodene er basert på vurderingene av det enkelte kriterie. Vurderingene er knyttet til de data som er samlet inn og som blir gjengitt i kapitlene nedenfor. Vi gjør derfor leseren oppmerksom på at vurderingene må sees opp imot de innhentede data i prosjektet.

| | | |
|---|---|---|
| | Kriterie 1 | Kommunen må kunne dokumentere at det er foretatt risikovurderinger knyttet til IT- og informasjonssikkerhet. |
| | Kriterie 2 | Kommunen må ha foretatt en vurdering av konsekvensene som brudd på personvern kan ha og en forhåndsdrøftelse av disse. |
| | Kriterie 3 | Kommunen må ha en informasjonssikkerhetsstrategi med målsettinger. |
| | Kriterie 4 | Kommunen må ha rutiner for autorisering, endring og avslutning av tilganger. |
| | Kriterie 5 | Kommunen må ha retningslinjer for privat bruk av informasjonssystemer og utstyr. |
| | Kriterie 6 | Kommunen må ha nødvendige rutiner og prosedyrer som sikrer tilfredsstillende håndtering av personopplysninger, og som oppdateres ved behov. |
| | Kriterie 7 | Kommunen må ha et avvikssystem som tilfredsstiller at avvik avdekkes, behandles, lukkes og som bidrar til avvik blir forebygget. |
| | Kriterie 8 | Kommunen må sikre avviksmeldinger som inneholder personopplysninger eller har betydning for informasjonssikkerheten. |
| | Kriterie 9 | Kommunen må ha identifisert hvilke personopplysninger de har. |
| | Kriterie 10 | Kommunen må ha fastsatt formål for behandlingen av personopplysninger. |
| | Kriterie 11 | Kommunen må føre protokoller over alle behandlingsaktiviteter. |
| | Kriterie 12 | Kommunen må på en kort og forståelig måte gi informasjon om hvordan de behandler personopplysningene. |
| | Kriterie 13 | Kommunen må ha et personvernombud og opplyse for ansatte og andre hvem personvernombudet er. |
| | Kriterie 14 | Kommunen må ha databehandleravtaler. |
| | Kriterie 15 | Kommunen må ha tiltak som sørger for tilstrekkelig kompetanse i organisasjonen vedrørende informasjonssikkerhet og personvern. |
| | Kriterie 16 | Kommunen må ha et tilfredsstillende system for informasjonssikkerhet og personvern. |

## 7.2 Innhentet data

### 7.2.1 Risikovurdering

Kommunestyret i Hamar kommune behandlet i februar 2022 kommunens ROS-analyse. Denne er gradert og unntatt offentlighet. I ROS-analysen er det to kapitler som er relatert til informasjonssikkerhet. Dette gjelder bortfall av ekom-løsninger og langvarig bortfall av strøm. Det blir i dokumentet vist til erfaringene fra Østre Toten, og hvert område blir risikovurdert. Det er ellers lite annet som går direkte på IKT og informasjonssikkerhet i ROS analysen.

Etter at Russland angrep Ukraina ble det sendt et felles brev fra KDD og KS til kommunedirektørene hvor det ble vist til at departementet ønsket at kommunene konsekvensutredet egen IKT-sikkerhet, i og med at Norges støtte til Ukraina kunne utløse cyberangrep fra russiskvennlige hackergrupper og militære cyberenheter. I forbindelse med brevet har kommunedirektøren og kommunedirektørens ledergruppe hatt en gjennomgang av status i Hamar kommune. Leder av IKT og utvikling utarbeidet i denne forbindelse en årsrapport for IKT sikkerhetsarbeid og sikkerhetshendelser i 2021, som lå til grunn for behandlingen i ledergruppen.

I rapporten blir det vist til:

- Status på Rett & rimelig-prosjektet i HIKT
- ROS og DPIA
- Opplæring IKT-sikkerhet
- Gjennomførte sikkerhetstiltak i 2021
- Innføringen av tilgangsportalen
- Statistikk, herunder informasjon om:
    - IKT-systemer og behandlinger
    - Teams
    - Internrevisjon (ikke gjennomført)
    - Sikkerhetshendelser
    - Uønskede hendelser og avvik i EQS
- Avvik sendt Datatilsynet
- Eksterne hendelser (Østre Toten og hva man kan lære av deres erfaringer)
- Vurderinger fremover, herunder
    - Prosedyre for databehandleravtaler
    - Informasjon om forvaltningsrevisjonen
- Forslag til aktiviteter, herunder:
    - To-faktor-autentisering ved pålogging Gat, elever og mobiler
    - Rydde i avdelingsstruktur og tilganger til filområder og Teams
    - Behov for felles løsning til sikkerhetsarbeid og personvern
    - Tilgangsstyringspolicy
    - Oppfølging av undersøkelse til kontrollutvalget
    - Følge opp KS sin anbefaling vedrørende Datasikkerhets- og beredskapstiltak i kommunal sektor

Ut over dette har vi fått informasjon om at kommunen ikke gjennomfører risikovurderinger spesifikt for informasjonssikkerhet og personvern.

Vi har fått opplyst at Hamar kommune gjennomfører risikovurderinger ved anskaffelser av nye systemer og applikasjoner, og ved vesentlige endringer i måten kommunen jobber på. Vi har også fått opplyst at kommunen mener at det er et forbedringspotensial på å gjennomføre risikovurderinger ved

endringer, og med hensyn til hvem som bør delta i disse risikovurderingene. Vi har fått oppgitt som et eksempel IKT-prosjekter hvor det er meningen å integrere løsninger i og mellom ulike fagsystemer.

Ved kommunalområdet opplæring og oppvekst er det etablert en kontroll ved anskaffelse av applikasjoner og programmer som skal benyttes i opplæringsøyemed. Hver anskaffelse skal starte med en forespørsel til rådgiverne ved opplæring og oppvekst. Den som sender forespørselen mottar et excel-ark med spørsmål knyttet til programvaren som skal anskaffes. Spørsmålene er knyttet til sikkerhet og personvern, og er todelt. Dersom man svarer ja på spørsmål i del 1 må det gjennomføres en risikovurdering. Dersom man svarer ja på spørsmål i del 2 må det gjennomføres en DPIA.

Vi har mottatt en utskrift av type behandlinger i Hamar kommune hvor det er gjennomført ROS og/eller DPIA. Det er totalt 144 behandlinger. For 31 av behandlingene er det gjennomført både ROS og DPIA. Det er samlet gjort 50 ROS-analyser og 33 DPIA-vurderinger.

DPIA er relevant med hensyn til risikovurderinger, men behandles i det påfølgende siden det stilles egne forventninger og krav til DPIA.

### 7.2.2 Vurderinger av konsekvenser ved brudd på personvern (DPIA)

Når man skal anskaffe og ta i bruk informasjonssystemer hvor personopplysninger vil bli behandlet, plikter man å foreta en vurdering av sannsynligheten for og konsekvensen av brudd på personvern. En slik vurdering kalles Data Protection Impact Assessment – forkortet DPIA. [7]

I møte har vi blitt vist et utvalg DPIA-vurderinger som er gjennomført i forbindelse med både anskaffelse av informasjonssystem og i forbindelse med aktiviteten informasjonsinnhenting (uthevet skrift). Vi ble vist DPIA for:

- **Innreiseregistrering/-oppfølging i forbindelse med covid-19**
- **Bekymringsmelding til barnevernet**
- Mercell
- Helseboka
- Remin

Hamar kommune har benyttet maler som er utarbeidet av andre virksomheter ved DPIA-arbeidet, blant annet av Bærum kommune og av KS Fiks. KS Fiks er en plattform for digitale fellesløsninger for kommuner og fylkeskommuner. [8]

Ut ifra malene må man i vurderingene beskrive

- systemet eller behandlingen,
- nødvendigheten og omfanget av datainnhenting og –behandling,
- hvordan data samles inn,
- hvor den behandles og lagres,

samt at det må foretas

- en konsekvens- og risikovurdering,
- vurderes risikoreduserende tiltak,
- utarbeides en rapport og til slutt forankre vurderingene hos ledelsen.

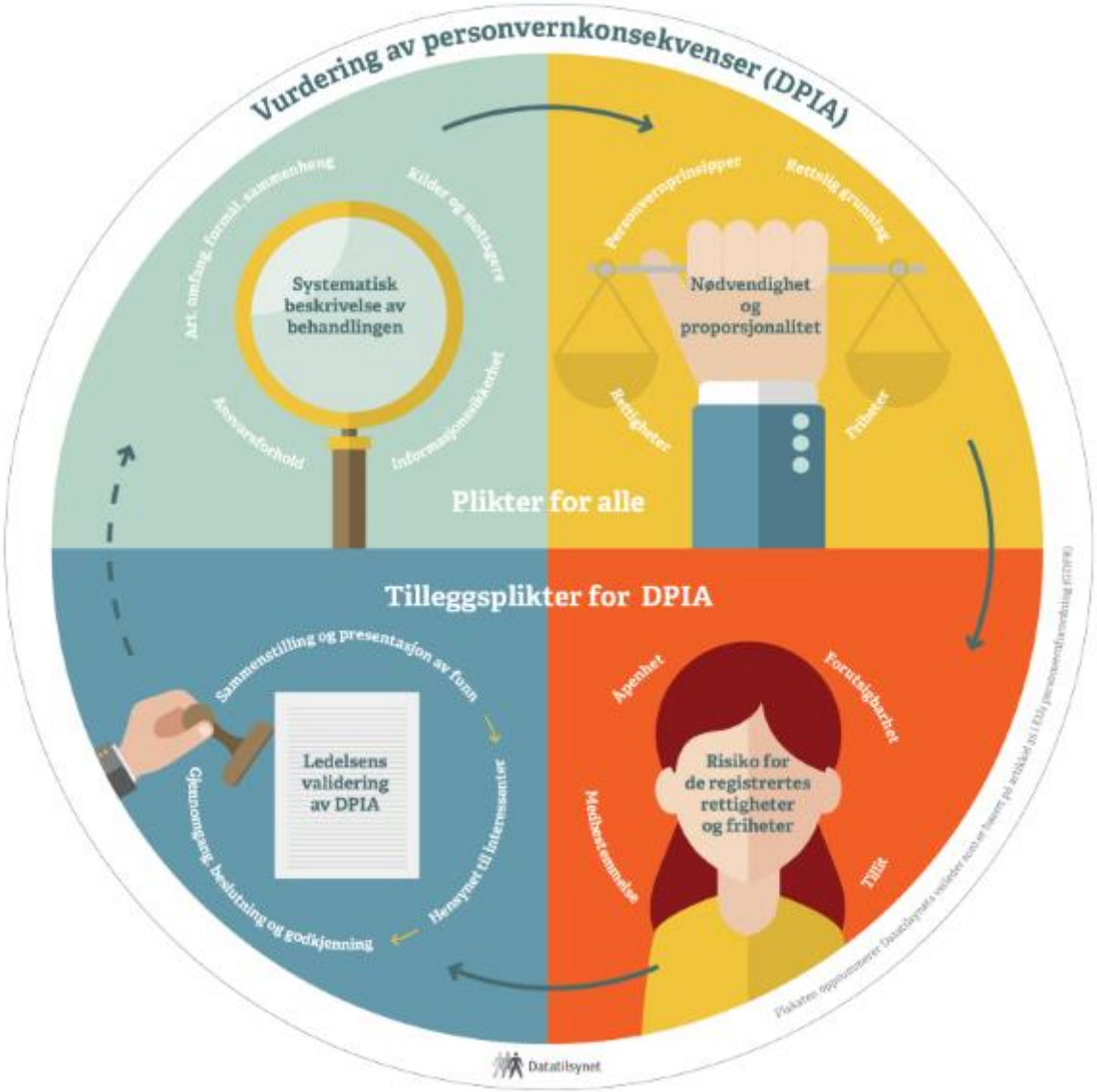
[7] Virksomheter er forpliktet til å gjennomføre en DPIA etter personvernforordningen (GDPR) artikkel 35.

[8] Kilde: https://www.ks.no/fagomrader/digitalisering/felleslosninger/fiks-plattformen/

Malene er todelte. Innledningsvis må man svare ja eller nei på innledende spørsmål. Dersom det er svart ja på minst to av spørsmålene må det utarbeides en utfyllende DPIA, jamfør samtlige av punktene ovenfor.

Av de fem DPIA-ene vi ble vist, var det en hvor utfyllende DPIA ikke var nødvendig. Av de øvrige fire valgte vi ut to som vi kontrollerte grundigere med hensyn til forankring i ledelsen. Dette gjaldt anskaffelse av løsning fra Mercell og behandlingen av informasjon ved bekymringsmelding til barneverntjenesten. De to DPIA-ene var utarbeidet etter maler.

Datatilsynet har utarbeidet følgende modell for plikter ved vurdering av personvernkonsekvenser:




*Figur 2: Kilde: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/hvordan-gjennomfore-en-dpia/*

Kommunen har også utarbeidet en sjekkliste til hjelp ved gjennomføring av DPIA. [9] Malene som Hamar kommune har benyttet, har felter hvor alle de ovennevnte pliktene inngår. I de to kontrollerte DPIA-ene er imidlertid steg 4 om ledelsens validering av DPIA ikke dokumentert. DPIA-ene er ikke påført

[9] Kilde: https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/dpia-veileder/sjekkliste-for-dpiafaser.pdf

ledelsens vurdering og signatur. Vi har fått opplyst at kommunalsjefen med ansvar for barnevernsområdet skal ha vært involvert i denne DPIA-en. I forbindelse med DPIA for Mercell har vi fått opplyst at det ikke var påtenkt at DPIA-ene skulle fylles ut og signeres av ledelsen.

I forbindelse med brevet fra KDD og KS, har det blitt tatt en beslutning i kommunedirektørens ledergruppe om at alle risikovurderinger knyttet til IKT og informasjonssikkerhet, inkludert DPIA-er, hvor risikovurderingen blir rød, skal kommunedirektøren godkjenne vurderingen. Dette ble bestemt den 10. mars 2022. Vi har imidlertid fått opplysning i en annen sammenheng om at dette administrative vedtaket er ukjent.

I forbindelse med gjennomgangen av DPIA-er hadde leder av IKT og utvikling funnet databehandleravtaler for to systemer som ikke var registrert med behandlingsansvarlig. Leder av IKT og utvikling var usikker på om disse to systemene er moduler i fagsystemer eller om de er å anse som egne systemer, og om hvordan disse skal registreres.

### 7.2.3 Informasjonssikkerhetsstrategi

Hamar kommune har en sikkerhetsstrategi med mål som ble vedtatt i kommunedirektørens ledergruppe i 2021, og er gyldig fra 7.1.21. Denne skal oppdateres i forbindelse med prosjektet Rett & Rimelig våren 2022, men selve dokumentet har en revisjonsfrist den 7.1.24. IKT sikkerhetsstrategien inneholder Hamar kommunes sikkerhetsmål. I denne strategien er målet:

> All informasjon som Hamar 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 Hamar kommune skal løse sine oppgaver og ha tillit hos innbyggerne.

Sikkerhetsstrategien beskriver videre at arbeidet skal forankres i øverste ledelse og inngå i ansvarsområdet som hver leder har til enhver tid. Deretter følger ni punkter for hvordan Hamar kommune ønsker at det skal være, med beskrivelse av hva Hamar kommune skal gjøre for å etterleve disse ønskene:

| **Slik vil Hamar kommune ha det** | **Slik gjør Hamar 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<br>• Informasjonssikkerhet og innebygd personvern – både teknisk og organisatorisk ivaretas før personopplysninger blir behandlet |
| **Informasjon kommer ikke på avveie (konfidensialitet)** | • Taushetsplikten respekteres<br>• Tilgang til informasjon er basert på tjenestlig behov<br>• 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:<br>• Bare produsert av de som har rett til det<br>• Ikke endret utilsiktet eller urettmessig<br>• 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<br>• Gir registrerte innsyn i egne opplysninger<br>• Gir mulighet til å rette, slette og flytte personopplysninger |
| **Respekterer innbyggernes personvern og deres rettigheter** | • Vi kjenner til og etterlever våre plikter og retningslinjer<br>• 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<br>• Avdekker feil som oppstår og lærer av dem<br>• 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<br>• Vi sikrer at vi ikke behandler personopplysninger ut over formål og lovlighet |

I forbindelse med at kommunens sikkerhetsarbeid skal forankres i ledelsen, så viser spørreundersøkelsen at 30 % av de som har svart opplever at ledelsen i liten grad har kommunisert forventinger til den enkeltes praktisering av digital sikkerhet.

Hamar kommune har i tillegg et dokument i EQS kalt sikkerhetsmål med gyldighet fra 27.9.13 og revisjonsfrist 20.9.17. I dokumentet fremgår det at dette er kommunens hovedmål. Målet er annerledes formulert enn målet i sikkerhetsstrategien, selv om innholdet i utgangspunktet er det samme. Dette målet er også gjengitt i andre rutinedokumenter som i utgangspunktet er utdaterte med hensyn til revisjonsfrist og lovhenvisninger:

> Hovedmål for informasjonssikkerheten i Hamar kommune er: sørge for at tjenestemottakere og ansatte er beskyttet mot hendelser knyttet til informasjonsbehandling som kan påvirke vår virksomhet eller vårt omdømme på en negativ måte.
>
> - **Konfidensialitet** – opplysninger ikke blir kjent for uvedkommende
> - **Tilgjengelighet** – alle med tjenestelig behov skal kunne utføre pålagte oppgaver
> - **Integritet** – opplysninger ikke endres uautorisert eller utilsiktet
> - **Autentisering** – personlig identifikasjon av den enkelte ansatt eller bruker
> - **Kvalitet** – alle opplysninger er korrekte og oppdaterte
>
> Informasjonssikkerheten skal kontinuerlig etterprøves og eventuelt forbedres. Medarbeiderne skal ha tilstrekkelig kompetanse og gis nødvendig opplæring slik at tilfredsstillende sikkerhet opprettholdes. Ved behandling av sensitive personopplysninger skal krav til tilgjengelighet vike for krav til konfidensialitet.

Vi har i tillegg til informasjonssikkerhetsstrategien mottatt et EQS-dokument kalt ansvar, roller og oppgaver. Dette dokumentet inneholder en beskrivelse av sikkerhetsorganisasjonen i Hamar kommune, og viser til funksjon, ansvar, rolle og oppgaver til den enkelte funksjon. Funksjonene som er nevnt er:

- Bruker
- Leder med personalansvar
- Kommunalsjef
- Kommunedirektør
- Personvernombud
- Leder IKT og utvikling
- Systemforvalter
- Hedmark IKT
- Sikkerhetsansvarlig Hedmark IKT
- Databehandlere

### 7.2.4 Autoriseringer og kontroll

HIKT har en egen tilgangsportal for bestilling av tilganger. Den enkelte leder med ansvar for bestillinger av tilganger må også sørge for at tilgangene lukkes. Tilgangsportalen er et skjema hvor man må krysse av for hvilke systemer man trenger eller ikke trenger tilganger til. Selve tilgangene må settes manuelt. HIKT setter tilganger i de systemene som de drifter og håndterer. Vi har i intervju imidlertid blitt gjort oppmerksomme på at NAV og Arkiv setter tilganger i egne systemer.

Arkiv har ansvar for ESA, som er kommunens sak- og arkivsystem. Ved arkiv er det to personer som har ansvar for å gi og lukke tilganger i ESA. Når ansatte trenger tilgang, må deres nærmeste personalansvarlige leder sende beskjed til arkiv for at tilgang skal gis. Dette er en praksis som med de siste årene har blitt strammet inn. Det var tidligere lettere for den enkelte bruker å selv bestille tilgang. ESA er gradert ut i fra arbeidssted og behov, slik at den personalansvarlige lederen må oppgi hvilke behov den ansatte har, og hva den skal ha tilgang til å lese og/eller endre.

Tilgangsportalen har erstattet praksis ved avslutting av tilganger. Tidligere fikk arkiv beskjed direkte fra personalansvarlig leder. Nå går dette gjennom tilgangsportalen. Arkiv mottar skjema fra HIKT om at en tilgang i ESA skal lukkes. Arkiv opplever at dette ikke er en optimal løsning. For det første opplever de at det er en del av skjemaene som gjelder ansatte som skal bytte arbeidssted internt i organisasjonen. Disse trenger sjelden å få tilgangene lukket, men omdefinert til nye behov. Dette medfører at arkiv må følge opp meldingen fra HIKT for å kontrollere mot kommunens register over ansatte.

Vi har fått oppgitt at tilgangene i ESA ikke blir systematisk gjennomgått, men at det blir gjennomført en kontroll med antallet tilganger. Hver enhetsleder mottar årlig liste over aktive bruker-identer i ESA og blir bedt om å oppdatere disse dersom oversiktene ikke stemmer. Vi har likevel fått oppgitt at det er en risiko for at ansatte som har jobbet lenge i kommunen kan sitte med tilganger som de har hatt i tidligere stillinger i kommunen. Det skal imidlertid, ifølge informasjon vi har fått, ikke være mulig å komme inn i ESA utenfor HIKT-nettet, slik at tilgangen til ESA vil avhenge av ansattstatus i lønnssystemet. ESA skal for øvrig fases ut og nytt sak- og arkivsystem skal etter planen tas i bruk høsten 2023.

Skolene i Hamar benytter Visma Flyt Skole. I systemet er det en rollebasert tilgangsstyring som synkroniseres opp mot Agresso, som er HRM-systemet i kommunen. Det finnes to administrator-roller, hvor den ene lar administratoren se og endre alt, mens den andre gir færre endringsrettigheter. Rektor og merkantilt ansatte har administratorroller. Disse blir satt og fjernet av opplæringskontoret.

Rektorene, og i noen tilfeller merkantilt ansatte med delegert myndighet, setter og fjerner roller overfor ansatte ved sin skole. Lærerne får roller som lærere, mens lærere med kontaktlæreransvar får en tilleggsrolle som kontaktlærer. Hensikten er at faglærere kun skal se informasjon om elever i sitt fag, mens kontaktlærere skal kunne få se all informasjon i alle fag for de elevene som de har ansvar for. Det finnes også noen øvrige roller som er av noe mindre betydning i det daglige, som for eksempel roller for lærere som jobber med eksamen. Systemet har også elev- og foreldreroller, med de begrensningene dette innebærer.

Visma Flyt Skole er ikke egnet som system for sikker saksbehandling. Opplæring og oppvekst har opplevd ulik praksis ved skolene opp igjennom årene. Ved noen skoler har saker blitt liggende i låsbare arkivskap, ved noen har det blitt liggende på passordbeskyttede minnepenner, og i flere tilfeller i senere tid har saker blitt lagt i ESA i egen mappe for den enkelte skolen. Dette gjelder saksbehandling knyttet til for eksempel spesialundervisning, særskilt språkopplæring og kapittel 9A-saker. Her har arkiv bistått med gradering av mappen slik at alt som legges der blir automatisk gradert, og kun de med riktig nivå på sin tilgang vil ha innsyn i mappen. Arkiv styrer disse tilgangene. Vi har fått informasjon om at disse tilgangene er svært begrenset, til det punktet at det har etablert seg løsninger som utløser andre utfordringer med hensyn til informasjonssikkerheten. Både kontakt- og faglærere kan ha behov for informasjon om særskilte vedtak. Siden disse ikke har tilgang i ESA, må en ansatt ved skolen med en slik tilgang skrive ut dokumentasjonen slik at læreren får den skriftlig. Dette introduserer en mulighet for at det som er skriftlig kommer på avveie. Det stiller også krav til hvordan det som er skriftlig blir arkivert når dokumentet ikke er i bruk, eller om det blir makulert.

I intervju har vi blitt fortalt at Opplæring og oppvekst er klare over at det er etablert en slik praksis og at dette ikke er ønskelig. Hamar kommune har derfor gjennomført en anbudsprosess og knyttet seg til en integrert løsning kalt Visma Flyt Sikker Sak, som skal kunne være enklere for skolene å håndtere med hensyn til informasjonsflyten av sensitive opplysninger. Systemet skal tas i bruk fra og med høsten 2022.

Hovedfagsystemet innenfor helsetjenestene er Gerica. Rollene i systemet blir satt på bakgrunn av bestilling fra leder med personalansvar. Tilgangene skal bestilles i Tilgangsportalen, og rollen skal defineres etter hva slags rolle den ansatte har ved det bestemte arbeidsstedet. Ansatte i helsesektoren kan har flere arbeidssteder, eller soner som det kalles innenfor helse. I disse tilfellene blir det satt en foretrukket sone for den ansatte. Den foretrukkede sonen er som regel den sonen den ansatte har størsteparten av sitt arbeidsforhold ved. Den ansatte må så bytte sone dersom den skal ha tilgang til informasjon fra annen sone. Rollen som gis begrenser hva og hvor mye informasjon den ansatte har tilgang til. Merkantilt ansatte har for eksempel ikke lesetilgang til helseopplysninger. Når ansatte har endring i kvalifikasjoner eller for eksempel mister en autorisasjon, må rollen endres manuelt. Dette introduserer en risiko for feil. Rollene i Gerica er ikke styrt opp mot lønnssystemet, så endret rolle i Agresso medfører ikke tilsvarende endring i Gerica.

Tilgangene i Gerica skal være satt opp slik at man har tilgang fem dager før og fem dager etter at en tjeneste skal gis. Siden helsetjenestene har plikt til å gi hjelp ved behov, eksisterer det også en nødhjelpstilgang i Gerica. Her kan et tjenestested gi seg selv tilgangen for å få innsyn i helseopplysninger til den som trenger bistand. Vi har fått opplyst at denne tilgangen som oftest benyttes av sykepleiere eller vernepleiere som har ansvar utover egen sone eller avdeling, eller får henvendelser om pasienter som på samme tidspunkt ikke mottar tjenester fra kommunen. Nødhjelpstilgangen følges av egne plikter for oppbevaring og loggføring på det som blir gjort med tilgangen, og tjenesteutøver må legge inn hva man har gjort og hvorfor. Det skal i etterkant kontrolleres om personen med tilgangen kun har gjort de handlinger som er lagt til grunn for å få tilgangen.

Det er i tillegg en funksjon i Gerica hvor ansatte kan gi seg selv nye pasienter og brukere. Dette gjelder korttids- og akuttavdelinger hvor man må kunne håndtere nye pasienter uten å måtte vente på saksbehandling og forarbeid. I slike tilfeller kan det også være behov for å benytte nødrettstilgangen.

Helse og omsorg opplever at det kan være feil i forbindelse med tilganger siden dette bestilles manuelt, men har inntrykk av at disse feilene som oftest omhandler at ansatte i korte engasjementer får sine tilganger lukket når leder har glemt å forlenge deres engasjementer. Systemansvarlig ga imidlertid uttrykk for at det kan være driftsmessige fordeler ved å sjekke tilgangene noe oftere enn det som gjøres nå.

NAV har flere systemer, som følger av tjenestebehov og arbeidsgiver, i og med at NAV er delt i henholdsvis kommunale og statlige oppgaver. Med hensyn til Lov om sosiale tjenester, hvor tjenestene og bistand er et kommunalt ansvar, benytter NAV Hamar systemet Socio. I tillegg har ansatte tilgang til ESA og til Hamar kommunes kvalitetssystem, EQS. For statlige tjenester har NAV et system for arbeidsrettet oppfølging, kalt Modia, et journalsystem for statlige tjenester kalt GoSYS, samt WebSak, og et avvikssystem for stat kalt Asys. Noen ansatte har i tillegg tilganger til eldre systemer som kun brukes unntaksvis og som er faset ut med hensyn til nye tjenester. Dette gjelder for eksempel Infotrygd som inneholder informasjon om yrkesskader og barnetrygd fra 1970-tallet, og Arena som inneholder journaler, men som er bestemt faset ut på grunn av GDPR og som kun brukes for oppslag.

Tilgangsstyringen ved NAV Hamar er todelt. HR-ansvarlig har ansvar for å legge til tilganger i et system kalt Remedy. Dette gjelder bestillinger av tilganger i de statlige systemene. For Socio er det oppnevnt to systemansvarlige, som setter og fjerner tilganger. Socio har både roller og sikkerhetsprofiler. Disse settes etter arbeidsområde og ansvar. Det er også anledning til manuelt, å begrense lese- og endringstilganger. For statlige systemer gis det tilgang etter tjenstlige behov. Felles for prosessen er at det er avdelingslederne som skal melde den ansatte behov med begrunnelse for hvorfor tilgangen skal gis.

Hvilke tilganger den enkelte ansatte skal ha varierer ganske mye. Alle ansatte i samme enhet har ikke nødvendigvis samme tilganger, fordi enkelte ansatte kan ha utvidet ansvar for oppfølging av særskilte grupper eller behov. Innenfor brukeroppfølging blir for eksempel en bruker veiledet av både en kommunalt og en statlig ansatt. Begge har tilganger til systemer innenfor kommunale og statlige oppgaver, men de kan ha ulike tilganger ut ifra rollen. Dette gjøres for at begge skal kunne gi god veiledning ut ifra hele tjenesteporteføljen til NAV.

Også andre kommunale tjenester benytter Socio, for eksempel flyktningtjenesten. Vi fikk opplyst at det tidligere var et utilfredsstillende skille mellom hvilken informasjon flyktningtjenesten og sosialhjelp hadde tilgang til. I begynnelsen av 2021 ble dette endret ved at det ble innført nivåinndeling på brukere av Socio. Nå har flyktningveiledere mindre tilgang til å se NAV-relatert informasjon, mens NAV-veilederne i avdeling Integrering har innsyn i informasjon om flyktningene. Samlet sett har alle NAV-ansatte fått innsyn i færre brukere gjennom nivådelingen.

Selv om det tilhører sjeldenhetene, er det anledning til å sette hastetilganger i systemene, innenfor samme prosedyre med hensyn til bestilling og begrunnelse. Systemene tillater også tidsavgrenset tilgang, som kan være nyttig ved ferieavvikling. Hastetilganger gis i større grad i de statlige enn de kommunale systemene. I forbindelse med slike tilganger forsøker NAV å forhindre at den ansatte blir sittende med roller som kan ha innvirkning på god forvaltningsskikk, for eksempel at samme ansatte ikke både fatter vedtak og godkjenner utbetalinger.

Vi ble fortalt at ved avgang lukkes tilgangene automatisk, men at det ikke er automatikk i stenging av tilganger ved skifte av avdeling, oppgaver og ansvar. Ved gjennomføringen av intervjuet var det to og

et halvt år siden sist NAV-kontoret hadde hatt en gjennomgang av tilgangene. Vi fikk opplyst at NAV Hamar i forbindelse med revisjonsprosjektet ser at de har et behov for å legge inn en slik gjennomgang i sitt årshjul.

### 7.2.5 Retningslinjer for privat bruk av informasjonssystemer og utstyr

I følge Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, som HIKT-kommunene har lagt til grunn for arbeidet i Rett og Rimelig, fremgår det at det er behov for retningslinjer for privat bruk av informasjonssystemer og utstyr. [10]

Vi har fått opplyst at kommunens datavettregler gjelder for privat bruk av informasjonssystemer og utstyr. I datavettreglene fremgår følgende som er relatert til privat bruk:

- Internett skal som hovedregel benyttes til arbeidsrelaterte oppgaver og i samsvar med kommunens etiske retningslinjer.
- Det er ikke tillatt å laste ned utuktig materiale, opphavsbeskyttet materiale (eks. film, musikk og programvare) eller annet som er i strid med gjeldende lover.
- Kommunen har via driftsleverandør anledning til å logge/lagre informasjon om internett- og e-posttrafikk i 7 dager for å sikre alminnelig drift samt for sporing ved eventuelle sikkerhetsbrudd
- Kommunens e-postsystem skal som hovedregel brukes til arbeidsrelaterte oppgaver og i samsvar med kommunens etiske retningslinjer og regelverk

I tillegg fremgår det at kommunen har kjøreregler for sosiale medier, og det fremgår at:

- På dine private profiler i sosiale medier er du privatperson. Vær bevisst på ikke å blande rollene privat og profesjonell/ansatt.

Datavettreglene inneholder ikke retningslinjer for bruk av privat utstyr, selv om mye av det samme vil være gjeldende. Vi har i spørreundersøkelsen og i intervju fått informasjon om at ansatte bruker private mobiltelefoner i jobbsammenheng både i skole og i helse og omsorg. Vi har også fått informasjon om at det kan være personopplysninger på disse telefonene.

### 7.2.6 Rutiner og dokumentasjon på vurderinger av nødvendige rutiner

Hamar kommune bruker kvalitetssystemet EQS som plattform for oversikt over alle prosedyrer, inkludert prosedyrer for informasjonssikkerhet og personvern.

Vi har fått oversendt flere av rutinedokumentene i EQS:

- Databrukeravtale, gyldig fra 5.1.21, revisjonsfrist 5.1.24
- Retningslinjer for mobilsikkerhet, gyldig fra 4.10.19, revisjonsfrist 3.10.22
- Datavett regler, gyldig fra 7.1.21, revisjonsfrist 7.1.22
- **Retningslinjer for sikkerhet ved bruk av IPAD, gyldig fra 14.2.12, revisjonsfrist 22.6.17**
- ***Opplæringskriv IKT-sikkerhet, gyldig fra 4.12.15, revisjonsfrist 3.12.17***
- ***Prosedyre for risikovurdering – personopplysninger, gyldig fra 7.6.10, revisjonsfrist 2.6.14***
- ***Prosedyre for informasjonsplikt ved innsamling av personopplysninger, gyldig fra 7.7.11, revisjonsfrist 1.7.14***
- ***Prosedyre – når personopplysninger er kommet på avveie, gyldig fra 25.4.13, revisjonsfrist 24.4.16***

[10] Normen, punkt 5.1. Kilde: https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren

- ***Håndtering av dokumenter med sensitivt innhold – prosedyre, gyldig fra 27.9.13, revisjonsfrist 26.9.16***
- **Bruk av bærbart utstyr – prosedyre, gyldig fra 3.8.15, revisjonsfrist 2.8.17**
- **Veiledninger personopplysninger i skolen – ressurser med lenker til veiledere fra Senter for IKT i utdanningen (disse lenkene er utdaterte og virker ikke lenger);**
    - **Sikker håndtering av personopplysninger i skolen**
    - **Sikker håndtering av personopplysninger ved bruk av skolens lagringsområde**
    - **Sikker håndtering av personopplysninger ved bruk av innloggingstjenester i skolen**
    - **Sikker håndtering av personopplysninger i forbindelse med spesialundervisning**
    - **Sikker håndtering av personopplysninger i det skoleadministrative systemet**
    - **Sikker håndtering av personopplysninger ved bruk av bærbar lærer-PC**
    - **Sikker håndtering av personopplysninger i den digitale læringsplattformen**

Rutinedokumentene i uthevet skrift har ikke blitt revidert innen kommunens egne revisjonsfrist, og alle disse er utarbeidet før EUs personvernforordning trådte i kraft i 2017. Dokumentene som også står i kursiv er dokumenter vi mener at har betydning for håndtering av personopplysninger etter GDPR.

Vi har fått opplyst fra Hamar kommune om at prosjektet Rett & Rimelig skal bidra til oppdateringer av gjeldende prosedyrer, men hvor man også prioriterer prosedyrer som alle HIKT-kommunene har potensial for å ha felles. I Rett & Rimelig har kommunene jobbet med å kartlegge behov for rutiner opp imot krav i normen for informasjonssikkerhet og personvern i helse- og omsorgssektoren. Vi har mottatt skjema som har blitt brukt i dette arbeidet. Her fremgår det en rekke behov, alt fra organisasjonskart med beskrivelse av ansvar og ROS-analyser til det mer konkrete med maler for bruk i det daglige. Følgende rutiner er nevnt i skjemaet:

- Rutiner for bruk av databehandler
- Rutine for verdiklassifisering av systemer
- Rutine for akseptabel risiko
- Rutine for gjennomføring og oppfølging av DPIA
- Rutine for gjennomføring og oppfølging av ROS
- Rutine for gjennomføring og oppfølging av overordnet ROS
- Rutine for bruk av behandlingsoversikt
- Rutine for opplæring
- Rutine for innsyn
- Rutine for reservasjonsrett
- Rutine for informert samtykke
- Rutine for informasjonsrett
- Rutine for retting
- Rutine for sletting
- Rutine for avviksrapportering
- Rutine for avviksbehandling
- Rutine for ledelsens gjennomgang
- Rutine for sikkerhetsrevisjon av kommunen
- Rutine for sikkerhetsrevisjon av enhet/avdeling
- IKT-instruks

### 7.2.7 Avvikshåndtering

Hamar kommune har både rutiner for generell avviksregistrering i EQS og spesielt med hensyn til personvern. Hvis bruddene på personvernet er alvorlige, skal det bli meldt avvik til Datatilsynet i egnet

kanal for dette. Rapporten for IKT-sikkerhetstiltak og –hendelser viser at 2 % av avvikene i EQS i 2021 var relatert til personvern og IKT-sikkerhet. 95 % av disse var meldt fra helse og omsorg, og 84 % av avvikene var knyttet til feilført journal. Vi har i intervju fått opplyst at feilført journal meldes som avvik på grunn av sikkerheten i Gerica. For å forhindre at informasjon urettmessig kan fjernes, må det sendes avviksmelding til systemansvarlig. Systemansvarlig må foreta korrigeringen. Journalen med feilføringen blir fortsatt arkivert ved endring, men journalen med feilføringen settes som inaktiv. På denne måten er kommunen sikret at det ikke er gått tapt informasjon, selv ved feilføring, og at kommunen kan dokumentere hvorfor endringen er gjort i journalen

Kommunen har meldt inn avvik til Datatilsynet, men har per 20. juni 2022 ikke blitt ilagt bøter fra Datatilsynet knyttet til avvikene. Det ble meldt kun ett avvik til Datatilsynet i 2021.

Spørreundersøkelsen viser for øvrig at en av fem ikke vet hvor eller til hvem de skal melde til ved digitale sikkerhetshendelser. De som har meldt har oppgitt at de i de fleste tilfeller vil melde fra til nærmeste leder og HIKT. Deretter følger leder av IKT og utvikling og enhetens lokale IKT-ansvarlige.

### 7.2.8 Fjerning av personopplysninger i avviksmeldinger

Hamar kommune benytter avviksmodul i EQS for registrering av avvik. Vi har fått en demonstrasjon av hvordan dette systemet fungerer. Det er et lederansvar å sørge for at eventuelle personopplysninger ikke ligger i avviksmeldingene. Vi har ikke fått informasjon som tilsier at dette er en stor utfordring i Hamar kommune. Av de kommunale tjenestene, kunne det ha vært helse og omsorg hvor personopplysninger mest sannsynlig kunne ha fulgt avviksmeldingene. Årsaken til dette skyldes at feilføringer i pasient- og brukerjournaler må meldes inn som avvik, fordi Gerica ikke tillater endring i systemet fra andre enn systemansvarlig. Dette for å sikre at helseopplysninger ikke forsvinner.

Under demonstrasjonen ble vi vist hvordan det er å registrere avvik i EQS dersom man jobber innenfor helse- og omsorgstjenestene. Den som fyller ut avviksmeldingen får informasjon om at meldingen ikke skal inneholde personopplysninger. I tillegg er det eget felt for å legge inn pasientens eller brukerens journalnummer, slik at mottaker ikke har behov for personopplysninger for å lete opp den aktuelle journalen i Gerica.

### 7.2.9 Identifisering av personopplysninger

Hamar kommune benytter et system utarbeidet av tidligere IT-ansvarlig i Løten kommune, kalt DP4000, for oversikt over personopplysninger, formål og behandlingsprotokoller. Vi har fått en demonstrasjon av systemet. Systemet har blitt endret for å ivareta kravene fra Arkivverket i forbindelse med arkivtilsyn i 2021.

Systemet inneholder oversikt over behandlinger, behandlingsansvarlig, formål og så videre. Det er to ansatte ved IKT og utvikling som har tilgang til systemet og som legger inn behandlingsoversikten. Noe av dette er kartlagt av IKT og utvikling, og noe er kartlagt ved samtaler med enhetsledere.

I kapittel 6 viser vi til at kommunen har vurdert at de har færre behandlingsprotokoller enn registrerte systemer, og at antallet behandlingsprotokoller skal være samme som eller høyere enn antallet systemer. Antallet systemer omtales også som sannsynligvis for lavt. Kommunen kan som helhet ha identifisert typer opplysninger til typer tjenester, men har ikke et oppdatert og helhetlig register over disse.

Vi har fått opplyst at identifiseringen av de opplysningene kommunen har er gjennomført ved IKT og utvikling, til dels i samtaler med sektor-/enhetsledere. I forbindelse med at kommunen skal skaffe seg et nytt GDPR-system, er det ønskelig at identifiseringen og registreringen av personopplysninger

gjennomføres i den enkelte enhet slik at de som er i praksisfeltet, og som kjenner oppgavene, selv kan føre oversikt over hva de har av personopplysninger, hva de brukes til og hvordan de behandles.

### 7.2.10 Formål for behandling av personopplysninger

For de personopplysningene som er kartlagt i forbindelse med behandlingsprotokoller i DP4000, er det lagt inn hva som er formålet med behandlingen. Det fremgår av prosedyre for informasjonsplikt ved innsamling av personopplysninger, dater 7.7.11, med revisjonsfrist 1.7.14, at tjenesten som samler inn personopplysninger på eget initiativ skal informere om formålet med behandlingen og hva opplysningene skal brukes til. Denne prosedyren er utdatert, og fremstår også som lite hensiktsmessig i og med at mange av tjenestene innhenter store mengder informasjon som en del av tjenesteytelsen. Det er lite sannsynlig at informasjon om formål blir gitt i hvert enkelt tilfelle.

Som vist til i kapittel 6 har kommunen færre behandlingsprotokoller enn registrerte systemer, og antakeligvis færre registrerte systemer enn hva som er kartlagt. Dette betyr i det minste at kommunen ikke har en sentral oversikt over formålene for behandlingen av personopplysningene for alle behandlinger, tilsvarende hva som ble omtalt i forrige underkapittel.

### 7.2.11 Behandlingsprotokoller

Årsrapporten for IKT-sikkerhetsarbeid og sikkerhetshendelser viser til at behandlingsprotokollene i DP4000 er langt færre enn registrerte systemer i Hamar kommune. Det blir videre vist til at antallet systemer antakeligvis er for lavt, og at antallet behandlinger skal være høyere enn antall systemer. Av dokumentet fremgår det at: «her er det et stort avvik og må tas tak i, det er behov for en løsning hvor behandlingsansvarlige selv kan oppdatere sine behandlinger».

I intervju har vi blitt opplyst om at leder av IKT og utvikling har fått i ansvar å anskaffe nytt GDPR-system for kommunene i HIKT-samarbeidet. Behovet for dette kom til syne i vurderingene av normen for informasjonssikkerhet. Kravspesifikasjon skal utarbeides høsten 2022, og utdraget fra rapporten som nevnt over kan bli en spesifikasjon i utlyst anbud. Det har allerede blitt gjennomført leverandørmøter, og kommunene håper at nytt system vil være på plass i begynnelsen av 2023.

### 7.2.12 Databehandleravtaler

DP4000 benyttes også som system for oversikt med databehandleravtaler. Databehandleravtaler avkreves der hvor andre enn kommunen selv behandler dataene. Dette kan for eksempel være at informasjonssystemene som brukes med tilhørende databaser ligger lagret på servere utenfor kommunen, eller for eksempel at det benyttes skyløsninger. Noen av fagsystemene i kommunen driftes av HIKT. I disse tilfellene er det HIKT som er databehandler. Hamar kommune har en generell databehandleravtale med HIKT for disse systemene. Det er ikke laget databehandleravtaler for hvert enkelt system.

For andre systemer som verken kommunen eller HIKT drifter, skal det være utarbeidet databehandleravtaler. Vi har mottatt en liste over 117 systemer. Av disse er det registrert databehandleravtale for 52 systemer. Av de 117 systemene er HIKT databehandler for 31. Det er krysset av for at det er databehandleravtale med HIKT for 30 av systemene.

Vi har i intervju fått informasjon om at kommunen ikke er sikre på om man har sentral oversikt over alle databehandleravtalene kommunen har for ulike systemer. Kommunen har for de 52 systemene nevnt over, hvorpå de store fagsystemene er inkludert. Men kommunen har også kommentert i årsrapporten for sikkerhetsarbeid og sikkerhetstiltak at de sannsynligvis mangler systemer i oversikten. I intervju med opplæring og oppvekst har vi fått opplyst at avtalene med de store fagsystemene ligger i ESA, men at avtaler for mindre systemer kan ligge arkivert andre steder.

### 7.2.13 Personvernerklæring

På Hamar kommunes nettsider ligger det ute en informasjonsside om personvern og bruk av e-post. [11] Nettsiden går ikke inn på tjenestenivå og de opplysninger som kommunen med bakgrunn i lov innhenter. I intervju har vi blitt fortalt at kommunen ikke har noen annen personvernerklæring enn den som ligger på kommunens hjemmeside. Det er ikke opprettet personvernerklæringer for den enkelte tjenesten i Hamar kommune.

I følge GDPR artikkel 13, skal en personvernerklæring inneholde:

- Identitet og kontaktopplysninger til behandlingsansvarlig (og eventuelt dennes representant)
- Kontaktinformasjon til personvernombud
- Formålene med behandling
- Rettslig grunnlag for behandling
- Lagring og oppbevaringstid
- Innsynsrett, rett til korrigering og til sletting, eller begrensning av behandling, protest mot behandling, rett til dataportabilitet
- Retten til å klage til tilsynsmyndighet

Vi har også sett på eksempler fra andre kommuner og fra andre offentlige instanser for å se hva de inkluderer i sine personvernerklæringer. I tillegg til kravene i artikkel 13, ser det ut til at det er vanlig å inkludere hva som samles inn av informasjon, og hvem informasjonen eventuelt deles med. [12]

Hamar kommunes informasjonsside om personvern og informasjonskapsler inneholder informasjon knyttet til brukere av nettsiden, men ikke om brukere av kommunale tjenester. Den inneholder også i liten grad informasjon knyttet til GDPR artikkel 13.

I løpet av revisjonsperioden har informasjonssiden blitt endret (publisert/sist endret 20.05.22). Nåværende informasjonsside inneholder mindre opplysninger enn den tidligere. I forbindelse med oppdateringen er den blitt mindre omfattende med hensyn til hvilke analyseverktøy som brukes. Det sto tidligere også at det føres liste over besøkende i rådhuset, samt om kamera i porttelefon. Dette er nå tatt ut. I tillegg er det fjernet informasjon om berørtes rettigheter og muligheter for innsyn, korrigering og sletting av data.

Informasjonssiden inneholder informasjon ved bruk av e-post, og at slik kommunikasjon er usikker. Brukere blir vist til at de kan sende sikker e-post gjennom ID-porten, med lenke til påloggingsside for løsningen. Det blir også informert om at man ikke sender e-poster med:

- Personnummer
- Opplysninger som kan knyttes til en selv eller andre
- Helseopplysninger
- Opplysninger om straffbar virksomhet
- Rasemessig eller etnisk bakgrunn
- Politisk, filosofisk eller religiøs oppfatning
- Helseforhold
- Seksuelle forhold
- Medlemskap i fagforeninger

[11] Kilde: https://www.hamar.kommune.no/hurtiglenker/personvern/

[12] Kilder: Ringsaker kommune, Bærum kommune, Målselv kommune, Stortinget, Helsedirektoratet, Forskningsrådet.

Avslutningsvis blir det vist til kommunens kontaktinformasjon, og navn og e-postadresse til kommunens personvernombud.

### 7.2.14 Personvernombud

Personvernombudets hovedoppgave er å informere om forpliktelsene som virksomheten har etter personvernlovgivningen. De skal også orienteres om beslutninger og gi råd i beslutningsprosesser med betydning for informasjonssikkerhet og personvern. Personvernet kan ha flere oppgaver, men dette avgjøres av den enkelte virksomhet.

Hamar, Stange og Løten har felles personvernombud. Personvernombudet sitter i HIKT sitt sikkerhetsråd. Kontaktinformasjonen til personvernombudet ligger ute på hjemmesiden til Hamar kommune. Det ligger også informasjon om personvernombudet på HIKT sin side over sikkerhetsansvarlige i HIKT. [13]

Den gjennomførte spørreundersøkelsen viser at få ansatte melder fra om hendelser til personvernombudet.

### 7.2.15 Opplæringstiltak

Spørreundersøkelsen viser at halvparten av de som har besvart undersøkelsen i liten grad har fått opplæring i digital sikkerhet. Et flertall av respondentene har også gitt uttrykk for at de ønsker mer opplæring. En fjerdedel oppgir at de ikke ønsker/har behov for mer opplæring.

De som ønsker opplæring ønsker opplæring innenfor:

- Digitale trusler
- Sikker bruk av e-post
- Hvordan behandle arbeidsrelatert informasjon på en sikker måte
- Varsling av sikkerhetshendelser i virksomheten

Spørreundersøkelsen viser også at opplæringstiltak har en viss effekt. For eksempel viser resultatene at ansatte med opplæring:

- opplever i større grad at ledelsen er gode rollemodeller for digital sikkerhet, og at de har kommunisert tydelig hvilke forventninger de har til sine ansatte
- er i større grad klar over at virksomheten har regler for digital sikkerhet
- er i større grad klar over hvem de skal melde fra til om digitale sikkerhetshendelser
- opplever i større grad at de er i stand til å vurdere hva som er trygt og utrygt å gjøre på nett, og mener i større grad at det er knyttet risiko til bruk av e-post, deling av jobb-passord med andre ansatte, bruk av sosiale medier, bruk av fysiske lagringsmedier, og bruk av sky-tjenester
- er i større grad bekymret for virus på arbeidsgivers datamaskiner, at utilsiktet feil vil kunne skade virksomhetens systemer, og mer bekymret for tap av data

Selv om undersøkelsen viser at mange ønsker mer opplæring, har vi mottatt dokumentasjon på og informasjon om opplæringstiltak generelt i kommunen, og innenfor sektorene og fagsystemene. Dette behandles i de påfølgende to underkapitlene.

[13] Kilde: https://www.hedmark-ikt.no/sikkerhet/sikkerhetsansvarlige/

#### *7.2.15.1 Generelle opplæringstiltak*

Hamar kommune har et dokument kalt «Opplæringskriv IKT-sikkerhet», gyldig fra 4.12.15 med oversittet revisjonsfrist 3.12.17. Dokumentet ligger tilgjengelig for alle ansatte i EQS. Opplæringsskrivet tar for seg informasjon om informasjonssikkerhet og personvern. Det inneholder også informasjon om:

- kommunens sikkerhetsmål,
- internkontroll,
- roller og ansvar, samt
- ansattes ansvar, herunder
    - gi informasjon,
    - fysisk tilgang og utforming,
    - IKT-systemer,
    - Bruker-identer,
    - tilgangskontroll og passord,
    - PC-er,
    - lagring av data,
    - programvare,
    - virus mv.,
    - overdragelse/destruksjon av lagringsmedia,
    - opplæring og
    - logging
- Lenke til datavettreglene
- Personvernbestemmelser
- Sikkerhetsarbeid

Dokumentet er som det tidligere er vist til, ikke oppdatert med hensyn til alle lovhenvisninger.

Under opplæring fremgår det at:

> «sikkerhetsopplæring gjennomføres for alle og inngår i kommunens introduksjonsprogram for nyansatte. God opplæring i bruk av programmer, vil være en viktig del av sikkerhetsarbeidet. Sikkerhetsreglene er en ramme rundt faglige gjøremål og kan vanskelig realiseres uten god kjennskap til oppgaver og rutiner. Den enkelte leder skal jevnlig vurdere opplæringsbehov sammen med medarbeider. Ut fra gjennomgang skisseres opplæringsbehov med begrunnelse og tidsaspekt».

De siste to årene med pandemi har bidratt til at det i liten grad er blitt gjennomført opplæring med informasjonssikkerhet som fokusområde.

I kapittel 6 er det nevnt at HIKT tilbød en opplæringspakke under nasjonal sikkerhetsmåned som er utarbeidet av NorSIS. Det var frivillig å delta og bare 2 % av de ansatte gjennomførte opplæringstilbudet. Måten e-posten var sendt på og så ut medførte imidlertid en del henvendelser og klager på at man hadde mottatt spam, så gjennomføringen fra leverandøren kan ha bidratt til lav deltakelse.

Da GDPR ble innført avholdt kommunen obligatorisk GDPR-kurs for alle ledere. Det ble gitt et tilbud om repetisjonskurs, som ble avlyst på grunn av for få påmeldte. Kommunen benytter KS læring som læringsplattform. KS læring har en rekke kurs på sine nettsider. [14] Per 20.6.22, ble 46 av kursene på siden tilbudt ansatte i Hamar kommune. Følgende kurs ble tilbudt innenfor informasjonssikkerhet:

[14] Kilde: https://www.kslaring.no/local/catalogue/index.php?facets=852&page=0&search=*

- Digital etisk refleksjon på Teams
- Opplæring HIKT Tilgangsportalen
- KiNS kurs – informasjonssikkerhet; kurset er modulbasert med følgende moduler:
    - Modul 1: Grunnleggende informasjonssikkerhet
    - Modul 2: Sikkerhet på mobile enheter
    - Modul 3: Trusler fra IT-kriminelle
    - Modul 4: Fysisk sikkerhet
    - Modul 5: Grunnleggende personvern
    - Modul 6: Utvidet personvern
    - Modul 7: Informasjonssikkerhet for ledere
    - Modul 8: Håndtering av sikkerhetshendelser
- KiNS kurs: Personvern og informasjonssikkerhet – filmer

Vi har i intervju fått opplyst at kommunens administrasjon generelt opplever at få ansatte tar kursene på KS læring.

I skjema vi har fått overlevert med kartlegging av behov i HIKT-kommunene i forbindelse med Rett & Rimelig-prosjektet, fremgår det at kommunene har behov for både en opplæringsplan og en opplæringsrutine.

#### *7.2.15.2 Opplæringstiltak i virksomhet/enhet/fagsystem*

Ansvaret for opplæring i ESA ble lagt over fra administrasjonen til arkiv i 2019. Vi har fått opplyst at systemet for opplæring ikke har vært godt nok, og at arkiv ikke har hatt tilstrekkelig med ressurser til å gjennomføre utstrakt grad av opplæring. Det har blitt opprettet en stilling som blant annet skal ha ansvar for å utarbeide opplæringsvideoer og –materiell for brukerne av ESA, og som skal drive opplæringstiltak i kommunen. En utfordring for den ansatte i stillingen er at ESA er et gammelt system som skal fases ut og som må erstattes, og at den nytilsatte selv har behov for opplæring i systemet før opplæringsmateriellet og –tiltakene kan gjennomføres.

I møte med NAV har vi fått opplyst at den nyansatte får en opplæringsplan ved oppstart. NAV har to sikkerhetsuker i løpet av året, henholdsvis vår og høst, hvor det gjennomføres opplæringstiltak innenfor informasjonssikkerhet og personvern. NAV stat sender ut egne eLæringsmoduler til ansatte, som må gjennomføres. Leder skal sjekke at hver ansatt har gjennomført eLæringen. Da GDPR ble innført avholdt Tieto, som leverer Socio, et to-dagers-kurs for ansatte ved NAV Hamar. Kurset var frivillig.

I helse og omsorg ligger ansvar for nødvendig opplæringstiltak til den nærmeste lederen i enheten. Dette gjelder både med hensyn til fagsystem og til informasjonssikkerhet og personvern. Systemansvarlig for Gerica kan bistå i å bestille kurs for hele avdelinger, eller at det avholdes spesielle kurs ved for eksempel endringer i lovverk eller andre føringer for saksbehandlingen. GAT som er et ressursstyringssystem og ledelsesverktøy i helsetjenestene, inneholder også en kompetansemodul for meldingsutveksling. Kompetansetiltakene er frivillige.

Innenfor skole og barnehage ble det gjennomført en omfattende opplæring da Visma-systemene ble innført. Vi ble i intervju imidlertid fortalt at generell opplæring i data og personvern har et forbedringspotensial. Informasjonssikkerhet og personvern er på agendaen i andre sammenhenger, for eksempel gjennom skolenes IKT-nettverk og nettverk for digitalpedagoger. Det blir også jevnlig tatt opp i skoleledernettverk. Vi ble likevel fortalt at opplæringen i informasjonssikkerhet og personvern mangler systematisering, og at Opplæring og oppvekst har vurdert økt bruk av KS læring sine eKurs. Vi ble opplyst om at Visma også har eLæringskurs innenfor forvaltningsrelatert taushetsplikt og

personvern. Ellers er det noen lærere som har denne kompetansen gjennom fag de underviser i og egeninteresse. Vi ble fortalt at nyansatte skal gjennomgå ansattopplæring, men at dette går mer på rutiner og førende dokumentasjon for den enkelte skole og for kommunen. Vi ble også fortalt at HR i Hamar kommune arbeider med et onboarding-program som skal ta utgangspunkt i KS læring, men at dette prosjektet er under etablering.

### 7.2.16 Styringssystem for informasjonssikkerhet og personvern

eForvaltningsforskriften § 15 stiller krav til at virksomheter har et tilfredsstillende system for informasjonssikkerhet og personvern, basert på en anerkjent standard på området. Det er ikke lagt føringer for hvilken standard kommuner skal bruke. Gjennom Rett & Rimelig har HIKT-kommunene valgt å ta utgangspunkt i Normen for informasjonssikkerhet og personvern i helse- og omsorgssektoren.

Det er utarbeidet et vedlegg til normen om hvordan normen forholder seg til lovverkene. [15] Her blir det vist til at eForvaltningsforskriften § 15 omtales i Normens kapittel 2.4, hvor det står om kravene til styringssystem. I normen blir det vist til at med styringssystem er det ment at man snakker om et internkontrollsystem, og dette handler om hvordan virksomheten planlegger, gjennomfører, evaluerer/kontrollerer og korrigerer etterlevelse av relevant regelverk, krav og avtaler.

I kapittel 3 har vi omtalt de tre «pilarene» som informasjonssikkerhet består av. Dette er:

- Styrende dokumenter – hvor det settes nivå for akseptabel risiko, IKT-reglement og informasjonssikkerhetspolicy.
- Gjennomførende dokumenter – hvor det lages rutiner for og gjennomføres IKT-anskaffelser, risikoanalyser, DPIA, opplæring og nødrutiner.
- Kontrollerende dokumenter – hvor man har rutiner for og gjennomfører avviksbehandling, sikkerhetsrevisjon og hvor ledelsen foretar en gjennomgang.

De styrende dokumentene er allerede omtalt i kapitlene:

- 7.2.1 Risikovurdering
- 7.2.3 Informasjonssikkerhetsstrategi
- 7.2.6 Rutiner og dokumentasjon på vurderinger av nødvendige rutiner

De gjennomførende dokumentene er omtalt i kapitlene:

- 7.2.1 Risikovurdering
- 7.2.2 Vurderinger av konsekvenser ved brudd på personvern (DPIA)
- 7.2.6 Rutiner og dokumentasjon på vurderinger av nødvendige rutiner
- 7.2.15 Opplæringstiltak

De kontrollerende dokumentene er omtalt i kapitlene:

- 7.2.7 Avvikshåndtering
- 7.2.13 Personvernerklæring
- Ledelsens gjennomgang er omtalt i flere kapitler knyttet til brev fra KDD og KS, og ble gjennomført i mars 2022.

[15] Kilde: https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren/Vedlegg%20Oversikt%20over%20Normens%20krav.docx

Vi har ikke omtalt nødrutiner, sikkerhetsrevisjoner og rutiner for IKT-anskaffelser tidligere. Rutiner for IKT-anskaffelser har vi ikke sett på i dette prosjektet.

Nødrutiner omhandler beredskap og hva man gjør dersom kritiske funksjoner for tjenesten bortfaller. Mye av dette handler om selve IKT-systemene, og ligger derfor utenfor avgrensningen mot HIKT. Vi har imidlertid mottatt en tiltaksplan ved langvarig bortfall av Ekom. Denne ble gjennomgått og oppdatert i ledergruppen i forbindelse med brevet fra KDD og KS. Tiltaksplanen inneholder vurderinger av hva som kan gå galt, sårbarheter, konsekvenser og tiltak, og generelle tiltak.

I dokumentet fremgår tiltak for hver tjeneste dersom Ekom bortfaller, og generelle tiltak. Innenfor generelle tiltak blir det blant annet vist til:

- Lokal reserveløsning for strøm
- Abonnement hos flere tilbydere med uavhengig kjernenett
- Reise til Kjonerud for å hente viktig informasjon som er lagret lokalt hos HIKT
- Tilgang til fagsystemer i annen HIKT-kommune dersom bortfallet er lokalt

Det har for øvrig blitt gjennomført beredskapstester med hensyn til bortfall av strøm og bruk av reserveløsning innenfor helse og omsorg, og i HIKT.

Med hensyn til sikkerhetsrevisjon, fremgår det av årsrapporten for IKT sikkerhetsarbeidet at det ikke har blitt gjennomført internrevisjon på sikkerhet under pandemien. I kapittel 7.2.6 har vi også nevnt at rutiner for sikkerhetsrevisjon er et kartlagt behov i Rett & Rimelig.

## 7.3 Revisors vurdering

### 7.3.1 Vurdering av revisjonskriterie 1 – Risikovurderinger

Hamar kommune har gjennomført noen risikovurderinger i sin ROS-analyse, som er knyttet til informasjonssikkerhet og IKT. ROS-analysen inneholder for eksempel vurderinger ved bortfall av ekom-løsninger og ved langvarige strømbrudd. Sistnevnte er relevant med hensyn til tilgang til tjenestekritisk informasjon.

En oversikt vi har mottatt viser at det er gjennomført ROS- og DPIA-vurderinger av en tredjedel av registrerte behandlinger og systemer. Årsrapport for sikkerhetsarbeidet i 2021 viser at det er risiko for at kommunen ikke har oversikt over behandlinger og systemer. Det er også mange andre momenter kommunen kunne ha vurdert med hensyn til risiko, for eksempel det som er knyttet til opplæring og til utdaterte rutinedokumenter. Det fremgår i samme årsrapport at det ikke er gjennomført sikkerhetsrevisjon. I en slik revisjon kunne risikomomenter ha kommet frem.

Vi har ikke fått dokumentasjon eller annen informasjon som tyder på at det er gjort en gjennomgående risikovurdering for disse områdene. Vi har heller ikke fått dokumentasjon som tyder på at kommunen har vurdert risiko-aksept.

Samlet sett mener vi at kravet til risikovurderinger innenfor informasjonssikkerhet og personvern bare er delvis etterlevd.

Kommunen må kunne dokumentere at det er foretatt risikovurderinger knyttet til IT- og informasjonssikkerhet.

### 7.3.2 Vurdering av revisjonskriterie 2 – Personvernkonsekvenser

Datatilsynet har utviklet en sjekkliste for DPIA. Vi har sett nærmere på to av fem av DPIA-ene. Den ene er tilfredsstillende innenfor tre av fire faser. Den fjerde fasen omhandler et personvernprinsipp om ansvarlighet. Dette prinsippet er ment ivaretatt ved at ledelsen har hatt befatning med vurderingene

og signert på at leder går god for vurderingene. Den andre DPIA-en har vi fått opplyst at kommunalsjef har behandlet. Kommunen har imidlertid ikke klart å dokumentere dette.

I Hamar kommune er det ingen rutine for gjennomføring av DPIA. Malene som har blitt benyttet er utviklet av Bærum kommune og av KS Fiks. Selv om vi ikke har mottatt dokumentasjon på at DPIA-ene er behandlet av en leder, betyr ikke dette at DPIA-ene ikke har blitt behandlet av/i ledelsen/ledergruppen. Men det vil være fordelaktig at kommunen sikrer at slik behandling blir dokumentert. Ledelsens gjennomgang av informasjonssikkerhet i Hamar kommune 10. mars 2022 viser imidlertid til at alle «røde» vurderinger skal til godkjennelse hos kommunedirektøren. Vi har fått informasjon som kan tyde på at denne beslutningen ikke har blitt distribuert til alle som deltar i slike vurderinger.

Selv om fase 4 ikke er gjennomført, mener vi likevel at revisjonskriterie 2 er etterlevd i det alt vesentligste, i og med at de viktigste vurderingene av personvernkonsekvensene er gjennomført.

Kommunen må ha foretatt en vurdering av konsekvensene som brudd på personvern kan ha og en forhåndsdrøftelse av disse.

### 7.3.3 Vurdering av revisjonskriterie 3 – Informasjonsikkerhetsstrategi

Hamar kommune har en IKT-sikkerhetsstrategi som inneholder et overordnet mål med delmål og beskrivelser på hvordan disse skal nås. IKT-sikkerhetsstrategien er i stor grad relatert til viktige momenter ved informasjonssikkerhet og personvern, og fremstår som tilfredsstillende.

Kommunen har også en oversikt over kommunens sikkerhetsorganisasjon.

Vi mener at revisjonskriterie 3 er etterlevd.

Kommunen må ha en informasjonsstrategi med målsettinger.

### 7.3.4 Vurdering av revisjonskriterie 4 – Rutiner for autorisasjoner

Våre undersøkelser viser at kommunen har rollestyrte systemer hvor brukere må være autorisert gjennom tilgangsstyring. Men undersøkelsene viser også at det kan være et behov for i større grad å systematisere en gjennomgang av tilgangene for å sikre at de som har autorisasjonen er berettiget til å ha denne. Undersøkelsene viser at dette gjelder spesielt i tilfeller hvor ansatte skifter ansvar og oppgaver internt i egen organisasjon.

Vi har blitt fortalt hvordan autorisasjoner og tilganger settes og fjernes i de de ulike fagsystemene, men vi har ikke mottatt skriftlige rutiner for hvordan dette gjennomføres. Vår oppfatning er at Hamar kommune har en tilfredsstillende praksis, men at kommunen blir sårbar ved eventuelle endringer overfor de som har ansvar for å sette på og fjerne tilganger. For å sikre det organisatoriske minnet mener vi at denne typen rutiner i størst mulig grad bør skriftliggjøres.

Vi mener derfor at revisjonskriterie 4 er delvis etterlevd.

Kommunen må ha rutiner for autorisering, endring og avslutning av tilganger.

### 7.3.5 Vurdering av revisjonskriterie 5 – Retningslinjer for privat bruk av informasjonssystemer og utstyr

Hamar kommune har noen retningslinjer for privat bruk av informasjonssystemer og utstyr i kommunens datavettregler. Vi savner imidlertid retningslinjer for bruk av privat utstyr. Informasjon i intervju og i spørreundersøkelsen tyder på at private telefoner blir brukt både i kontakt med elever, foreldre, brukere og pasienter, og at det blir tatt opp medier av disse i ulike sammenhenger. I slike

tilfeller er Normen klar på at virksomheten skal sørge for at slike opplysninger fjernes. Dette fordrer at kommunen har innført rutiner for hvordan dette skal håndteres.

Vi mener at revisjonskriterie 5 er delvis etterlevd.


Kommunen må ha retningslinjer for privat bruk av informasjonssystemer og utstyr.

### 7.3.6 Vurdering av revisjonskriterie 6 – Oppdaterte rutiner for håndtering av personopplysninger

Den gjennomførte spørreundersøkelsen viser at en fjerdedel av de som har besvart undersøkelsen ikke kjenner til virksomhetens regler for digital sikkerhet.

Hamar kommune har flere rutiner for håndtering av personopplysninger, men disse rutinene er utdaterte i den forstand at de har passert intern revisjonsfrist, og at de ikke har blitt oppdatert til verken GDPR eller ny personvernlov. De ligger også i kvalitetssystemet, og undersøkelsen reiser spørsmål om hvorvidt rutinedokumentene blir brukt i og med at mange mener de er ukjente.

Selv om rutinene ikke er oppdaterte, er imidlertid flere av punktene i rutinene tilsvarende kravene i personvernlovgivningen slik de er i dag. Men det er også flere av rutinene som har feil lovhenvisninger og lenker til nettsider som ikke lenger finnes.

Skjema fra Rett & Rimelig viser at HIKT-kommunene har dokumentert et behov for forholdsvis mange rutiner, som i dag enten mangler eller er utilstrekkelige.

Til tross for dette, skal rutinene sikre at kommunen etterlever regelverket, noe som forutsetter at de er utformet deretter.

Vi mener derfor samlet sett at revisjonskriterie 6 ikke er etterlevd, og det fremstår som at det er behov for en opprydding i rutinene.


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

### 7.3.7 Vurdering av revisjonskriterie 7 – Avvikssystem

Hamar kommune har etter vår vurdering et tilfredsstillende avvikssystem i EQS. Systemet lar ansatte registrere avvik. Avviket går til og behandles av nærmeste leder.

Vi mener at revisjonskriterie 7 er etterlevd.


Kommunen må ha et avvikssystem som tilfredsstiller at avvik avdekkes, behandles, lukkes og som bidrar til avvik blir forebygget.

### 7.3.8 Vurdering av revisjonskriterie 8 – Sikring av avviksmeldinger med personopplysninger

Sikringen av at personopplysninger ikke fremgår av avviksmeldingen må gjennomføres av den lederen som mottar avviket. Vi har fått oppgitt at leder har mulighet til å fjerne eventuelle personopplysninger dersom dette er lagt inn i det meldte avviket.

Det skal imidlertid ikke være behov for å legge inn personopplysninger i et avvik. Dersom et avvik, eksempelvis i helse og omsorg, blir meldt inn og avviket omhandler en pasient, så er det et felt i registreringen hvor den som melder kan legge inn pasientjournalkode, slik at mottaker av avviket ikke må søke opp eventuell bruker eller pasient med annen personinformasjon.

Vi mener at revisjonskriterie 8 er etterlevd.

Kommunen må sikre avviksmeldinger som inneholder personopplysninger eller har betydning for informasjonssikkerheten.

### 7.3.9 Vurdering av revisjonskriterie 9 – Identifisering av personopplysninger

Hamar kommune bruker et lokalt utviklet system for oversikt over personopplysninger kalt DP4000. Leder av IKT og utvikling har i stor grad ansvar for å legge inn informasjon i dette systemet. Også en annen ansatt ved IKT og utvikling har tilgang. Noe informasjon om personopplysninger er hentet inn gjennom samtaler med enhetsledere.

Ansvaret for å kartlegge og registrere behandling av personopplysninger er i seg selv fordelt på en slik måte at det er risiko for at ikke alle behandlinger blir kartlagt. Dette skyldes at mye ansvar er lagt til få personer, som dermed må ha kontroll på og kontakt med forholdsvis mange kommunale områder for å være sikre på at alt i systemet er riktig.

Vi har blitt vist en oversikt av systemet, men ut fra denne er det ikke mulig å si noe om kommunen har klart å kartlegge alle personopplysninger. Kommunen har selv i årsrapport for sikkerhetshendelser beskrevet at kommunen sannsynligvis mangler oversikt over både systemer og behandlinger. Da er det også sannsynlig at det mangler identifisering av opplysningene som samles inn.

Anskaffelsen av et nytt GDPR-system vil kunne bidra til å forbedre denne prosessen og redusere risikoen for at noe i kartleggingen er avglemt. Vi har fått opplyst at det er ønskelig at mer av ansvaret legges ut til virksomhets- og enhetsledere, hvor de selv må opprette behandlingsprotokoller for de behandlingene de gjennomfører hos seg. Dette gjør oversikten mer praksisnær. Dette kan også bidra til bedre kvalitetskontroll. På den andre siden avhenger det av god opplæring av lederne.

Vi mener at revisjonskriterie 9 er delvis etterlevd, i og med at kommunen ikke kan garantere for at kommunen har full oversikt.

Kommunen må ha identifisert hvilke personopplysninger de har.

### 7.3.10 Vurdering av revisjonskriterie 10 – Formål for behandling av personopplysninger

Tilsvarende vurderingen for forrige kriterie, er det sannsynlig at kommunen ikke har oversikt over formålet for behandlinger av alle personopplysninger. Dette må sees opp imot revisjonskriterie 12 om personvernerklæring, i og med at kommunen plikter å oppgi formål for behandling av alle personopplysninger.

Vi mener at revisjonskriterie 10 er delvis etterlevd.

Kommunen må ha fastsatt formål for behandlingen av personopplysninger.

### 7.3.11 Vurdering av revisjonskriterie 11 – Behandlingsprotokoller

Kommunen har oversikt over behandlingsprotokoller i DP4000, men dette systemet har ikke full oversikt over alle behandlinger. Som vist til i årsrapport for sikkerhetsarbeid 2021, så mangler kommunen flere behandlinger målt opp mot det antallet systemer som er registrert i DP4000. Det blir også vist til at antallet systemer antakeligvis er lavere enn hva som er reelt.

Vurderingen av revisjonskriteriet avhenger også av vurderingene for revisjonskriterie 9 og 10. Det samme som er nevnt over med hensyn til anskaffelse av GDPR-system vil også gjelde for behandlingsprotokollene, særlig med hensyn til en delegering av oppgaven om å kartlegge hva hver enkelt enhet har og gjør med sine personopplysninger.

Vi mener at revisjonskriterie 11 er delvis etterlevd.

Kommunen må føre protokoller over alle behandlingsaktiviteter.

### 7.3.12 Vurdering av revisjonskriterie 12 – Personvernerklæring

I løpet av forvaltningsrevisjonen har Hamar kommune endret sine nettsider. Tidligere lå det ute en noe mer omfattende personvernerklæring på kommunens nettsider. Denne er nå nedskalert, og den enkeltes rettigheter er for eksempel tatt ut.

Vår oppfatning er at Hamar kommunes personvernerklæring ikke tilfredsstiller kravene i GDPR artikkel 13, og er vesentlig mindre omfattende enn øvrige kommuner og offentlige virksomheter sine, som vi har vist til tidligere i teksten.

Vi mener at revisjonskriterie 12 ikke er etterlevd.

Kommunen må på en kort og forståelig måte gi informasjon om hvordan de behandler personopplysningene.

### 7.3.13 Vurdering av revisjonskriterie 13 – Personvernombud

I kommunens personvernerklæring fremgår informasjon om og kontaktinformasjon til kommunens personvernombud. Informasjonen er med andre ord tilgjengelig både for ansatte og for innbyggere i kommunen.

Resultatet fra undersøkelsen reiser spørsmål ved om personvernet er kjent blant ansatte i organisasjonen. Men undersøkelsen viser at kommunen har lagt ut informasjon om hvem personvernombudet er.

Vi mener at revisjonskriterie 13 formelt sett er etterlevd.

Kommunen må ha et personvernombud og opplyse for ansatte og andre hvem personvernombudet er.

### 7.3.14 Vurdering av revisjonskriterie 14 – Databehandleravtaler

I forbindelse med kontrollen har vi funnet at kommunen mangler oversikt over databehandleravtalene. Dette gjør det utfordrende å kontrollere for hva som eventuelt mangler. Dette har også sammenheng med at man mangler fullstendig oversikt over alle systemer, samt at det kan være databehandleravtaler som er arkivert andre steder enn ESA. Kommunen hadde imidlertid oversikt over databehandleravtalene med fagsystemene som vi har kontrollert for.

Vi mener at revisjonskriterie 14 er delvis etterlevd.

Kommunen må ha databehandleravtaler.

### 7.3.15 Vurdering av revisjonskriterie 15 – Opplæringstiltak

Den gjennomførte spørreundersøkelsen viser at halvparten ikke har mottatt opplæring. Kommunen har både generelle tiltak for opplæring og tiltak i både sektorer, virksomheter og i fagsystemet. Opplæringstiltakene og –tilbudene er imidlertid i liten grad systematisert. Det fremstår for oss som at det er frivillig å løfte egen kompetanse.

I Rett & Rimelig har HIKT-kommunene kartlagt at de har behov for en kompetanseplan. Vi har også fått oppgitt at den enkeltes behov skal kartlegges i møter mellom leder og ansatte. Vi har blitt fortalt at det går an å gjøre opplæringstiltak obligatoriske, men undersøkelsen tyder på at dette i liten grad benyttes. Unntaket gjelder kravene som stilles i Nav stat, som også kan gis kommunalt ansatte i Nav, hvor ledere må påse at obligatoriske digitale kurs er gjennomført.

Hamar kommune har et forbedringspotensial for å sikre bedre kompetanse om informasjonssikkerhet og digital kompetanse i egen organisasjon. Vi har fått opplyst at HR arbeider med et onboarding-program som skal sørge for opplæring av nyansatte. Deltakelsen i spørreundersøkelsen viser imidlertid at mange som deltok har arbeidet mange år i kommunen og har oppgitt at de i liten grad fått opplæring. Det er derfor også behov for påfyll underveis i arbeidsforholdet. Det er ingenting som tilsier at dette behovet vil bli noe mindre fremover.

Vi mener at revisjonskriterie 15 er delvis etterlevd.

Kommunen må ha tiltak som sørger for tilstrekkelig kompetanse i organisasjonen vedrørende informasjonssikkerhet og personvern.

### 7.3.16 Vurdering av revisjonskriterie 16 – System for informasjonssikkerhet og personvern

I vurderingen av om Hamar kommune har et tilfredsstillende system for informasjonssikkerhet og personvern, er det naturlig å sikte til behovet for å ha styrende, gjennomførende og kontrollerende dokumenter.

Vi har i revisjonskriterie 1 vist til at kommunen ikke har dokumentert at man har gjennomført risikovurderinger for informasjonssikkerhet og satt nivå for akseptabel risiko. Kommunen har IKT-reglement, men mange av rutinene er utdaterte, som vi har omtalt i revisjonskriterie 6. I revisjonskriterie 3 har vi vurdert at kommunen har en IKT-sikkerhetsstrategi, som svarer opp hva som vil være naturlig å inkludere i en informasjonssikkerhetspolicy.

Vi har ikke sett på rutiner for og gjennomføring av IKT-anskaffelser og nødrutiner, så dette vurderer vi ikke. Men vi har i revisjonskriterie 1 vurdert risikoanalyser, i revisjonskriterie 2 vurdert DPIA, og i revisjonskriterie 15 vurdert opplæring.

Rutiner for og gjennomføring av avviksbehandling har vi vurdert i revisjonskriterie 7 og 8, sikkerhetsrevisjon er omtalt i tilknytning til revisjonskriterie 1 og nevnt i forbindelse med Rett & Rimelig, og ledelsens gjennomgang er nevnt i forbindelse med brev fra KDD og KS.

Ut ifra våre tidligere vurderinger, fremstår det for oss som at kommunen tilfredsstiller kravene til informasjonssikkerhetsstrategi og avvikssystem, men at det øvrige enten er delvis eller ikke tilfredsstillende.

Samlet sett er vi av den oppfatning av at kommunen har et forbedringspotensial for å etterleve kravet til et tilfredsstillende system for informasjonssikkerhet og personvern. Samtidig vil vi understreke at det for tiden pågår et arbeid med å forbedre mange av disse momentene innenfor Rett & Rimelig-prosjektet, særlig med hensyn til rutiner og planer som man har kartlagt et behov for. Kommunen har også visse ting på plass, for eksempel nevnte strategi med målsettinger og avvikssystem.

Vi mener samlet sett at revisjonskriterie 16 er delvis etterlevd.

Kommunen må ha et tilfredsstillende system for informasjonssikkerhet og personvern.

# 8 Konklusjon

I dette forvaltningsrevisjonsprosjektet har vi kontrollert Hamar kommune for overordnede styringsprinsipper for informasjonssikkerhet og personvern. Dette er i stor grad knyttet til kommunens internkontroll på området, men også til praksis. Undersøkelsen har bestått av dokumentstudier, intervjuer og demonstrasjon av fagsystemer og avvikssystem, samt gjennomføring av en omfattende spørreundersøkelse.

Vår overordnede problemstilling har omhandlet om kommunen har etablert en god sikkerhetskultur i organisasjonen. I sikkerhetskultur legger vi at man har overordnede føringer som ligger til grunn for en god praksis. Vi har vurdert forholdsvis mange krav og forventninger som stilles til kommunen.

Vi har funnet at Hamar kommune har et forbedringspotensial knyttet til:

- Risikovurderinger for informasjonssikkerhet
- Rutiner for DPIA
- Rutiner for endring og avslutning av tilganger, og gjennomgang av autorisasjoner
- Rutiner for bruk av privat utstyr og sikring av at personopplysninger på privat utstyr blir slettet ved opphør av arbeidsforhold
- Identifisering av personopplysninger, formålet for behandling og oversikt over hva og hvordan opplysninger blir behandlet
- Oversikt over databehandleravtaler
- Opplæringstiltak

Vi har funnet at Hamar kommune ikke har:

- Utarbeidet nødvendige rutiner og prosedyrer for håndtering av personopplysninger
- Sørget for at rutinene og prosedyrene blir oppdatert til interne frister
- Utarbeidet tilfredsstillende personvernerklæring
- Sikret at kommunens system for informasjonssikkerhet og personvern tilfredsstiller en anerkjent standard iht. eForvaltningsforskriften § 15.

Vi har på den andre siden funnet at kommunen har en tilfredsstillende informasjonssikkerhetsstrategi, et tilfredsstillende avvikssystem og at man har et personvernombud.

**Samlet sett mener vi at Hamar kommune har et forbedringspotensial med hensyn til å etablere en sikkerhetskultur, noe vi mener starter med selve styringssystemet, herunder risikobasert internkontroll.**

Informasjon vi har mottatt i intervjuer tyder imidlertid på at det er mange prosesser i gang. Rett & Rimelig-prosjektet består av flere momenter som skal lede frem til at deltagerkommunene, for eksempel får på plass en tilfredsstillende GDPR-løsning, og at man får koordinerte rutiner ut ifra de behovene som er kartlagt i prosjektet.

Vi har også fått informasjon i intervjuer knyttet til begrensninger i fagsystemer som øker risiko for feil. Dette gjelder for eksempel Visma Flyt Skole hvor informasjon knyttet til særskilte vedtak ligger i en gradert mappe i ESA, slik at ledelsen ved skolen må skrive ut informasjonen på papir når lærere har behov for den. Et annet eksempel er ESA, som er i ferd med å bli faset ut av leverandør og hvor kommunen nå får begrenset brukerstøtte. På skole skal det imidlertid fases inn et supplerende system som skal bidra til at nåværende praksis opphører, mens det er i gang en prosess for å finne en erstatningsløsning til ESA. Et tredje eksempel er tilfeller hvor det blir tatt bilder av sår og brukere/pasienter i helse- og omsorgstjenesten for å sikre at andre regelverk etterleves med hensyn

til dokumentasjon og medisinhåndtering. Slike bilder blir ikke arkivert på tilfredsstillende måte fordi fagsystemet ikke har tillatt lagring av bilder. Vi har imidlertid fått informasjon om at en modul i Gerica-systemet som sikrer arkivering av bilder knyttet til pasientjournal vil bli faset inn.

# 9 Anbefalinger

Vi har følgende anbefalinger til Hamar kommune:

- Kommunen må sikre et tilfredsstillende system for informasjonssikkerhet og personvern. Dette innebærer:
    - Systematiske og dokumenterte risikovurderinger for informasjonssikkerhet
    - Dokumenterte vurderinger for akseptabel risiko
    - Utarbeide nødvendige rutiner for informasjonssikkerhet og personvern, og holde disse oppdatert, inkludert rutine for DPIA som forsikrer forankring i ledelsen
    - Utarbeide opplæringsplan med hensyn til informasjonssikkerhet og personvern
    - Planlegge og gjennomføre sikkerhetsrevisjoner
    - Ta stikkprøver innenfor informasjonssikkerhet og personvern i forbindelse med internkontrollen
- Kommunen bør sørge for at det blir foretatt jevnlig gjennomgang av og kontroll med tilganger i fagsystemene.
- Kommunen må sikre at personopplysninger blir slettet fra private medier ved opphør av arbeidsforhold, når arbeidsforholdet forutsetter bruk av privat medium, som for eksempel mobiltelefon.
- Kommunen må utarbeide en tilfredsstillende personvernerklæring som gjøres kjent for kommunens ansatte og innbyggere.
- Kommunen bør gjøre rutinene kjent i organisasjonen.

# 10 Kommunedirektørens uttalelse

## Kommentar til forvaltningsrevisjonsrapport – informasjonssikkerhet

Funnene i rapporten stemmer stort sett slik tilstanden er i kommunen.

Generelt er ansatte i kommunen er bevisst viktigheten av personvern og informasjonssikkerhet, men det er et behov for mer opplæring og at rutiner oppdateres i hht nytt regelverk. Kommunen deltar årlig i nasjonal sikkerhetsmåned og informasjonssikkerhet og personvern er ofte innebakt i generell opplæring i fagsystem.

Det interkommunale prosjektet «Rett & rimelig» har som målsetting å bidra til en mer effektiv måte å få oppdatert prosedyrer og oversikter som kreves deriblant behandlingsoversikt. Samarbeid om ROS og DPIA vil gjøre det enklere å få dette på plass i enheter når kommunen har begrenset kapasitet på området. Prosjektet er nå i prosess med anskaffelse av et felles system for informasjonssikkerhet og GDPR. Aktivitetene i prosjektet vil bidra til å lukke avvikene i rapporten.

I tillegg foregår det mange aktiviteter på nasjonalt nivå. KS har satt i gang arbeidet med å utvikle et opplæringsløp innen informasjonssikkerhet for kommunalt ansatte «Nasjonal program for IKT sikkerhet i kommunal sektor (NPISK)».

# 11 Referanser

Hamar kommune

2010. Prosedyre for risikovurdering – personopplysninger

2011. Prosedyre for informasjonsplikt ved innsamling av personopplysninger

2012. Retningslinjer for sikkerhet ved bruk av IPAD

2013. IKT sikkerhetsmål

2013. Håndtering av dokumenter med sensitivt innhold – prosedyre

2013. Prosedyre – når personopplysninger er kommet på avveie

2015. Bruk av bærbart utstyr – prosedyre

2015. Opplæringsskriv IKT-sikkerhet

2019. Retningslinjer for mobilsikkerhet

2021. Datavett regler

2021. Ansvar, roller og oppgaver (sikkerhetsorganisasjonen i Hamar kommune)

2021. IKT sikkerhetsstrategi

2021. Databrukeravtale

2022. Rapport over databehandleravtaler (fra DP4000)

2022. Rapport over ROS-analyser og DPIA (fra DP4000)

2022. Møtereferat fra ledelsens gjennomgang 10.3.22

2022. Notat til kommunedirektør, datert 21.3.22, vedr. status og svar på KS sitt brev til landets kommunedirektører og ordførere 09.03.22

Udatert. Tiltaksplan ved langvarig bortfall av ekom

Udatert. Årsrapport IKT sikkerhetsarbeid og sikkerhetshendelser i 2021

HIKT

Udatert. Dokumentkart informasjonssikkerhet. Rett & Rimelig.

Udatert. Prosjektbegrunnelse og prosjektforslag konseptfase. Anskaffelse av GDPR-system.

Heggernes, T. A. 2020. *Digital forretningsforståelse. Fra store data til små biter (3. utgave).* Fagbokforlaget

KS. 2022. *Sikkerhetstiltak i norske kommuner i forbindelse med Russlands invasjon av Ukraina*. https://www.ks.no/globalassets/fagomrader/digitalisering/personvern-og-informasjonssikkerhet/Sikkerhetstiltak-i-norske-kommuner-i-forbindelse-med-Russlands-invasjon-av-Ukraina.pdf

## 11.1 Internettreferanser

Datatilsynet – Sjekkliste for DPIA:

- https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/dpia-veileder/sjekkliste-for-dpiafaser.pdf

Direktoratet for e-helse – Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren:

- https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren

Direktoratet for e-helse – Vedlegg – Oversikt over Normens krav:

- https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren/Vedlegg%20Oversikt%20over%20Normens%20krav.docx

Hamar kommune – Personvern:

- https://www.hamar.kommune.no/hurtiglenker/personvern/

Hedmark IKT – Sikkerhetsansvarlige:

- https://www.hedmark-ikt.no/sikkerhet/sikkerhetsansvarlige/

KS Fiks:

- https://www.ks.no/fagomrader/digitalisering/felleslosninger/fiks-plattformen/

KS Læring:

- https://www.kslaring.no/local/catalogue/index.php?facets=852&page=0&search=*

# 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 problemstillingen(e), 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, mål, føringer og lignende, 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 kriteriene og gis anledning til å komme med innspill.

## Bakgrunn for bestillingen

I henhold til kommuneloven § 23-2, punkt c, skal kontrollutvalget 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 (§ 23-3, første ledd).

Kontrollutvalget i Hamar kommune la inn informasjonssikkerhet som del av sin plan for forvaltningsrevisjon og eierskapskontroll 2020-2023, vedtatt av kommunestyret i møte 24. februar 2021 (sak 12/21). Kontrollutvalget igangsatte undersøkelser av temaet gjennom orienteringer fra Hedmark IKT og kommunedirektøren, først i møte 9. mars 2021 (sak 16/21), deretter den 8. juni 2021 (sak 30/21).

Den 9. mars 2021 bestilte kontrollutvalget en forundersøkelse/prosjektplan rettet mot temaet informasjonssikkerhet (sak 16/21). Forundersøkelsen ble lagt frem i møtet den 8. juni (sak 32/21). Kontrollutvalget ønsket å gå videre med planleggingen av prosjektet og ga Revisjon Øst IKS i oppdrag å legge frem en revidert prosjektplan i møte den 7. september (sak 49/21). I dette møtet fattet kontrollutvalget følgende vedtak:

4. Revisjon Øst IKS bes om å gjennomføre forvaltningsrevisjonsprosjektet i tråd med den fremlagte planen.
5. Formålet med et forvaltningsrevisjonsprosjekt om sikkerhetskultur er å se etter om Hamar kommune har sikret en god sikkerhetskultur i organisasjonen og hvordan kommunen håndterer avvik relatert til informasjonssikkerhet. Revisjonsprosjektet skal besvare følgende problemstilling:
    a. Har kommunen etablert en god sikkerhetskultur i organisasjonen, herunder internkontroll for personvern og informasjonshåndtering, og avvikshåndtering?
6. Revisjonsprosjektet gjennomføres innenfor en timeramme på 350 timer med sannsynlig levering i april/mai 2022.

# Utledning av revisjonskriterier

**Problemstilling:**
Har kommunen etablert en god sikkerhetskultur i organisasjonen, herunder internkontroll for personvern og informasjonshåndtering, og avvikshåndtering?

I det følgende utledes kriteriene som er planlagt benyttet i forvaltningsrevisjonsprosjektet. Utledningen er en gjennomgang og drøfting av hva krav og anbefalinger har å si for forventningene til praksis. Prosjektets problemstilling har, slik vi tolker det, to temaer:

- Internkontroll for personvern og informasjonshåndtering
- Avvikshåndtering

I behandlingen av bestillingen har kontrollutvalget ytret ønske om at forvaltningsrevisjonsprosjektet tar for seg kommunens kultur for informasjonssikkerhet og personvern. Det er vanskelig å stille krav til en kultur. En kultur består både av nedfelte regler som overleveres skriftlig eller muntlig, og av uuttalte og implisitte normer for handling og tankesett. Det som er skriftlig er vesentlig enklere å kontrollere enn det som overleveres muntlig, og begge deler er enklere å stille krav til enn det som ligger implisitt til grunn for handlinger.

I prosjektet har vi valgt å foreta en avgrensning mellom det som gjelder teknisk drift, og det som kommunen drifter, ivaretar og kontrollerer selv av tjenester og systemer. Mye av det som går på informasjonssikkerhet ligger til tekniske løsninger som Hedmark IKT (HIKT) drifter etter en samarbeidsavtale mellom kommunen og HIKT. Dette faller utenfor kontrollen. Vi vil i stedet kontrollere hvordan informasjonssikkerhet håndteres i organisasjonen med hensyn til atferden i disse tekniske løsningene. Dette velger vi å kalle *informasjonshåndtering*. [16]

KS har utgitt en veileder til kommunedirektørens internkontroll, kalt *Orden i eget hus*. Veilederen skal være til hjelp for kommunene for å føre internkontroll i praksis, etter gjeldende regler i kommuneloven. I tillegg, har KS gitt ut et tillegg til kommunedirektørens internkontroll som går konkret inn på informasjonssikkerhet og personvern. KPMG har hatt arbeidet med å utarbeide dokumentet, og definerer sikkerhetskultur på denne måten:

> *«Organisasjonens sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og adferd som kommer til uttrykk gjennom virksomhetens totale ivaretagelse av informasjonssikkerhet og personvern. En viktig forutsetning for å bygge en kultur hvor informasjonssikkerhet og personvern ivaretas er «tonen på toppen». Kommunedirektøren og kommunens øvrige ledelse bør derfor sette temaet på kommunens agenda, og selv gjennom det man sier og gjør være gode sikkerhetsforbilder».* [17]

I dette dokumentet har vi valgt å først fokusere på det som er generelle krav til kommunedirektørens internkontroll. Deretter vil vi komme inn på lovkrav med hensyn til det som gjelder informasjonshåndtering og **personvern**, og så hvilke anbefalinger som gjelder for de to områdene. Vi vil så komme inn på avvikshåndtering, og så Hamar kommunes egne rutiner på området. Disse rutinene

[16] Helse- og omsorgsdepartementet har brukt samme begrep i et rundskriv for spesialisthelsetjenesten mht. grensegangene mellom taushetsplikt, personvern og informasjonssikkerhet. Kilde: https://www.regjeringen.no/no/dokumenter/rundskriv-i-32019-om-informasjonshandtering-i-spesialisthelsetjenesten/id2642049/

[17] Kilde: KS/KPMG. 2022. Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet. Et tillegg til Kommunedirektørens internkontroll – Orden i eget hus. Side 33.

er naturlige å legge til grunn i kontrollen, siden de er fastsatt for hele organisasjonen og skal være toneangivende for atferden i kommunens informasjonssystemer.

## Generelt om internkontroll

Kommunedirektørens internkontroll er regulert i kommunelovens internkontrollbestemmelse i § 25-1. Det mest sentrale ved internkontrollen er at:

- Internkontrollen skal sikre at lover og forskrifter etterleves i alle ledd i organisasjonen,
- den skal være systematisk og tilpasses virksomhetens størrelse, egenart, aktiviteter og risikoforhold,
- den skal være risikobasert ved at det må gjennomføres konkrete risikovurderinger, som må gjennomføres på alle organisasjonsnivåer,
- avdekkede risikoforhold må følges opp med internkontrolltiltak, som for eksempel rutiner og prosedyrer, og
- internkontrollsystemet skal kunne bidra til å avdekke og legge grunnlag for å korrigere avvik.

Kommunal- og moderniseringsdepartementet (KMD) utga høsten 2021 en veileder til de rettslige forholdene til internkontrollbestemmelsen. [18] Departementet vurderer internkontrollbestemmelsens innhold som en minstebestemmelse. Internkontrollen kan inneholde mer enn det minimum som bestemmelsen beskriver, men dette må i hvert tilfelle vurderes ut ifra kommunens behov.

En kommunes internkontroll består av overordnede risiko- og vesentlighetsvurderinger på ulike nivåer i organisasjonen, dokumentasjon av vurderinger og tiltak, rutiner og prosedyrer for å redusere risiko og å sikre regeletterlevelse, kontrolltiltak og tilbakemeldinger fra praksisfeltet (avviksmeldinger, oppfølging og evaluering). I KMDs veileder blir det vist til at en i forarbeidene til kommuneloven har omtalt at dokumentasjonen og omfanget av dokumentasjon må sees i forhold til hva som er nødvendig for at kommunen skal kunne drive tilfredsstillende internkontroll, herunder sikre regeletterlevelse. [19] Men det blir også vist til at dokumentasjon er viktig for å sikre at internkontrollen fungerer som forutsatt, og at det ofte vil være naturlig å skriftliggjøre flere elementer ved internkontrollen, som for eksempel rutiner og prosedyrer. [20] Dette betyr at det ikke er dokumentasjonskrav for alt som et internkontrollsystem skal omfatte, likevel skriver KMD også at mange aspekter ved internkontrollen vil være nødvendig å dokumentere.

Vi mener at det vil være naturlig å forvente at kommunen kan dokumentere risiko- og vesentlighetsvurderinger, i og med at disse vil være førende for hva som er nødvendig for at kommunen skal kunne oppfylle internkontrollbestemmelsen. De rutiner og prosedyrer som kommunen skriftliggjør vil ha et behov for oppdateringer jamfør eventuelle avvik som avkrever forbedring, og ved endringer i lov- og regelverk. [21] Eksempler på situasjoner som vil kunne avkreve rutiner og prosedyrer er i de tilfeller hvor det stilles krav til at man kan dokumentere at lov og forskrift er ivaretatt, tjenesteområder og arbeidsoppgaver hvor man enten er avhengig av nøkkelpersoner eller hvor det er høy turnover, hvor man må sikre at alle handler likt for å etterleve regelverk, eller hvor lov- og regelverk fremstår som komplekst eller hvor reglene ikke implisitt ligger til fagopplæringen for de som må ivareta regelverket i de daglige tjenestene.

[18] Kilde: https://www.regjeringen.no/contentassets/961e9a785fb34a4d95be4cf2b9cc4c33/veilder-internkontroll_november-2021.pdf

[19] Ibid.: side 17.

[20] Ibid.: side 16 og 18.

[21] Ibid.: side 18.

Digitaliseringsdirektoratet (Digdir) har laget en ressursside om krav og anbefalinger til internkontroll på informasjonssikkerhetsområdet. [22] Her fremgår blant annet referanser til eForvaltningsforskriften § 15, som pålegger forvaltningsorganer å ha et internkontrollsystem for informasjonssikkerhet. Digdir skriver at dette kravet bør ivaretas gjennom helhetlig arbeid med styring og kontroll, og som en integrert del av virksomhetens helhetlige styring. Digdir viser også til at lovverket forutsetter en risikobasert tilnærming til informasjonssikkerhet, i likhet med det øvrige internkontrollkravet til kommunen i kommunelovens internkontrollbestemmelse.

eForvaltningsforskriften § 15 går videre ved å stille krav til at offentlige forvaltningsorganer utarbeider både mål og en strategi for informasjonssikkerhet. Dette vil ofte inngå i det samme dokumentet. Digdir viser til at en informasjonssikkerhetsstrategi bør inneholde:

1. retningslinjer for hvordan sikkerhetsarbeidet skal organiseres og gjennomføres (roller, myndighet, ansvar)
2. retningslinjer for relevante tiltaksområder

Digdir skriver at eForvaltningsforskriften legger føringer for at kommunen benytter anerkjente standarder for styringssystem for informasjonssikkerhet, og viser til at de selv anbefaler at offentlige og private virksomheter legger NS-ISO/IEC 27001 til grunn. Hamar kommune har ikke lagt denne til grunn for sine systemer, men har valgt, sammen med HIKT og øvrige kommuner i samarbeidet, å legge til grunn Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren for hele kommunen (også bare kalt *Normen*). [23] Normen er også å anse som en anerkjent standard.

KS har utarbeidet en veileder for kommunedirektørens internkontroll, kalt *Orden i eget hus*. [24] KS sin veileder er ment å være en veileder for internkontroll i praksis. I tråd med kommuneloven, er veilederen fokusert på risikobasert internkontroll. Fire av ti kapitler omhandler risiko.

I henhold til kommuneloven skal internkontrollen dokumenteres etter hensiktsmessig form og nødvendig omfang. KS mener det er opplagt at kravet om dokumentasjon gjelder rutiner og prosedyrer, risikoanalyser, iverksatte tiltak og avvikshåndtering m.m. [25] Hvordan dette er dokumentert kan variere. KS viser til at det i enkelte tilfeller kan være nok å vise til konklusjonen og vurderinger fra risikoanalysen. Andre ganger er det nødvendig å dokumentere andre former for underlag, tiltaksbeskrivelser, strategi og planverk osv.

KS viser til at de tre sentrale elementene i et godt internkontrollsystem er risikovurderinger, formalisering og kontrollaktiviteter. Risikovurderinger har vi forklart ovenfor. Med formalisering mener KS behovet for og praksisen ved å formalisere en organisasjon med ansvar og roller, utvikling av dokumentasjon, rutiner og prosedyrer, og sammenstilling og rapportering i systemet. Innenfor kontrollaktiviteter viser KS til at man bør gjennomføre stikkprøver og planlagte og faste kontroller, drive avvikshåndtering, og at dette gjennomføres både daglig og faglig.

Med bakgrunn i dette mener vi at det er naturlig å forvente at Hamar kommune kan dokumentere at det er foretatt risiko- og vesentlighetsvurderinger knyttet til IT- og informasjonssikkerhet. Vi mener også at man bør forvente at kommunen har en sikkerhetsstrategi og en fastsatt rolle-/ansvarsdeling i organisasjonen for sikkerhetstiltak. Kommunen bør også kunne dokumentere vurderingene av hvilke

[22] Kilde: https://www.digdir.no/informasjonssikkerhet/regelverkskrav-og-anbefalinger-internkontroll-informasjonssikkerhet/3229

[23] Kilde: https://www.ehelse.no/normen

[24] Kilde: https://www.ks.no/link/bb26f349bfba413abd465621fc61f4d5.aspx

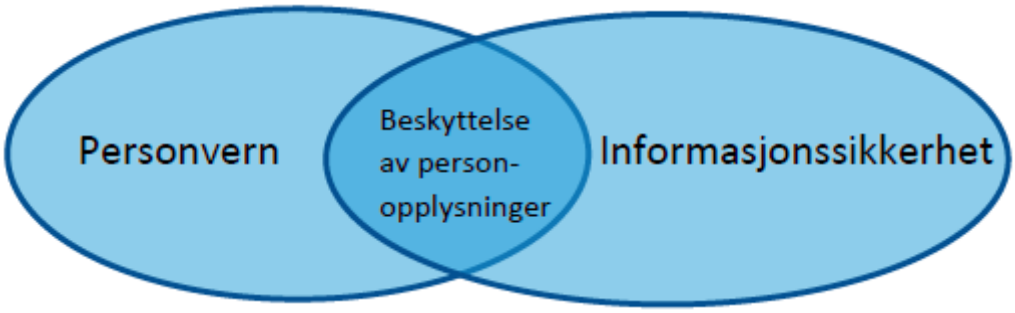
[25] Kilde. KS. 2021. Orden i eget hus. Side 45.

rutiner og prosedyrer som er nødvendige for å sikre regeletterlevelse innenfor informasjonssikkerhet og personvern, at disse rutinene og prosedyrene er utarbeidet, og at rutinene og prosedyrene holdes oppdaterte/vedlikeholdt.

## Anbefalinger for informasjonssikkerhet og personvern

KS ga i 2022 ut et tillegg til kommunedirektørens internkontroll. [26] Dokumentet er utarbeidet av KPMG og skal fungere som en verktøykasse for kommunedirektører for temaene informasjonssikkerhet og personvern.

KPMG viser i dokumentet til at GDPR og ny personvernlovgivning visker ut noen av forskjellene mellom informasjonssikkerhet og personvern. Samtidig viser de også til at informasjonssikkerhet og personvern er to forskjellige fagområder med overlappende temaer. Følgende modell benyttes for å skissere at personvern og informasjonssikkerhet overlapper der hvor det omhandler beskyttelse av personopplysninger:




Dokumentet inneholder en rekke anbefalinger til hvordan kommunedirektøren best kan ha kontroll med kravene til informasjonssikkerhet og personvern.

De første anbefalingene handler om å skaffe seg oversikt over hva man har av informasjon og opplysninger, og kategorisere disse etter hva slags verdi de har. Inndelingen som KPMG viser til er ikke en mal, men et eksempel på hvordan dette kan gjøres. KPMG deler først inn informasjonen i ulike verdinivåer med hensyn til hvor viktig informasjonen er for tjenesteytelsen i kommunen:

- Kritisk verdi
  - Informasjon som er kritisk i en krisesituasjon.
- Høy verdi
  - Informasjon som vil være ødeleggende for funksjoner og tjenester som er kritisk for daglig drift.
- Middels verdi
  - Informasjon som kan skade kommunens tjenester og funksjoner.
- Lav verdi
  - Åpen informasjon uten særskilte sikkerhetsbehov.

KPMG skriver at det etter en slik gjennomgang vil være naturlig å starte med den informasjonen det er knyttet størst negativ risiko til. Disse vurderingene skal ende opp i en tiltaksplan. Tiltaksplanen må inneholde hvem som er ansvarlige for det enkelte tiltak og hvilke risikovurderinger som er gjort. Risikovurderingene bør i tillegg kobles opp til den sektorovergripende internkontrollen. I denne internkontrollen bør kommunen vurdere hvor ofte man bør kontrollere tiltakene i forbindelse med evaluering av om iverksatte tiltak fungerer etter hensikten.

[26] Kilde: https://www.ks.no/link/550b6847994842b5bc1247a65f8f2cf3.aspx

KPMG skriver at det er ulike sikkerhetstiltak knyttet til om risikoen er relatert til informasjonssikkerhet eller personvern. Informasjonssikkerhetstiltak er ofte knyttet til teknisk drift. Dette er tiltak som for Hamar kommune skal ivaretas av Hedmark IKT gjennom felles samarbeidsavtale. KPMG skriver imidlertid videre at god informasjonssikkerhet og personvern også avhenger av gode arbeidsrutiner og sikkerhetsbevissthet hos de ansatte. Dette kan for eksempel dreie seg om tilgangsstyring, internkontroll, opplæringstiltak og adgangskontroll til fysiske bygg og gjenstander. Andre momenter som kan være viktige er retningslinjer for bruk av sosiale medier, bruk av samme passord over flere plattformer, eller bruk av samme passord både privat og på jobb m.m.

Vi mener at det er naturlig å forvente at kommunen kan dokumentere at det er foretatt vurderinger av hvilke typer informasjon kommunen bør prioritere å sikre, og at det er iverksatt tiltak basert på disse prioriteringene.

### Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen)

Normen for informasjonssikkerhet og personvern i helse- og omsorgssektoren ble vedtatt 4. februar 2020, og er tatt i bruk av kommunene i HIKT-samarbeidet, inkludert Hamar kommune. Normen inneholder noen minstekrav for å sikre at virksomheter ivaretar taushetsplikten og at uvedkommende får kjennskap til opplysninger (konfidensialitet), at informasjon er sikret mot utilsiktet eller uautorisert endring eller sletting (integritet), at informasjon er riktig og tilgjengelig for de som trenger den (tilgjengelighet og robusthet). De viktigste punktene er: [27]

- Tilgang til systemene må avgrenses til autorisert personell i henhold til tjenstlige behov. Dette innebærer at kommunen må ha rutiner for autorisering, endring og avslutning av tilganger for ansatte i tjenestene.
- Loggføring av alle som har hatt tilgang til personopplysninger og annen informasjon av betydning for informasjonssikkerheten.
- Loggføring av hvem som har rettet, registrert, endret og slettet opplysninger.
- Tiltak som sikrer at personopplysninger føres på rett person, i henhold til relevant kodeverk og terminologi, og at opplysningene er korrekte og oppdaterte.
- Tiltak som sikrer tilgjengelighet til systemene, og som muliggjør forebygging, deteksjon, skalerbarhet, håndtering og gjenoppretting.

Normen inneholder også et eget kapittel som omhandler medarbeidere, kompetanse og holdningsskapende arbeid. Her fremgår det blant annet at virksomheten bør ha en instruks for informasjonssikkerhet og personvern som omfatter de vesentligste kravene. Dette kan inngå som en del av opplæringen av de ansatte, som vi vil komme tilbake til i kapitlet om avvikshåndtering. Hamar kommunes instruks blir også omtalt i kapitlet om kommunens rutiner.

Normen legger føringer for at virksomheten skal ha retningslinjer for privat bruk av informasjonssystemer og utstyr. Virksomheten skal også ha tiltak som sikrer tilstrekkelig kompetanse for alle som gis tilgang til informasjonssystemene og tilhørende informasjon. Kompetansen omhandler både bruk av systemer og for å ivareta informasjonssikkerheten. Det er anbefalt at man fører oversikt over den enkeltes kompetanse og behov for opplæring.

Vi mener det er naturlig å legge alle disse momentene til grunn som forventninger til Hamar kommune.

## Lovkrav for personvern

[27] Kilde: https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren#3.2%26nbsp%3BMinimumskrav%20for%20%C3%A5%20sikre%20konfidensialitet%2C%20integritet%2C%20tilgjengelighet%20og%20robusthet

GDPR og personvernloven stiller noen krav til hva kommunen må ha på plass for å sikre den enkeltes personvern. Noen av de mest sentrale kravene er at:

- Kommunen må ha et personvernombud som er uavhengig virksomhetens ledelse. Det bør være tydelig kommunisert til organisasjonen hvem dette er.
- Kommunen må gjennomføre risikovurderinger for behandlinger (DPIA). Dette innebærer at man også kartlegger og identifiserer hvilke personopplysninger kommunen har.
- Dersom behandlingen innehar høy risiko for de registrertes rettigheter og friheter, og tiltak ikke vil redusere risikoen, må kommunen rådføre seg med Datatilsynet før behandlingen starter, i en såkalt *forhåndsdrøftelse*. En forhåndsdrøftelse er en skriftlig, formalisert prosess. [28]
- All behandling av personopplysninger skal føres i en egen oversikt, også kalt behandlingsprotokoller. Kommunen må angi formålet for behandlingen av personopplysningene.
- Kommunen må gi innbyggerne informasjon om hvordan personopplysninger behandles. Vanligvis gis dette i en personvernerklæring, og det er anbefalt at den er både kort og forståelig.
- Det skal inngås felles behandlingsansvarsavtaler når kommuner har samarbeid med andre, f.eks. statlige organer.
- Det skal inngås databehandleravtaler når kommuner bruker eksterne leverandører som behandler personopplysninger på vegne av kommunen.
- Kommunen må ha et internkontrollsystem for å ivareta alle pliktene i personopplysningsloven.

Alle disse punktene er naturlige å stille som krav til kommunen på personvernområdet.

## Avvikshåndtering

I internkontrollbestemmelsen er det tatt inn at internkontrollsystemet skal bidra til å avdekke og følge opp avvik og risiko for avvik. For at systemet skal kunne avdekke avvik, må det være noen klare føringer for hva som er å anse som avvik. Dette kan for eksempel være basert på risikovurderinger hvor man har identifisert eksempler på avvik, eller hvor man har prosedyrestyrt tjenestevirksomhet hvor alt som ikke inngår i prosedyren er å anse som et avvik. Hva som er et avvik i den enkelte tjeneste vil med andre ord variere.

Vi har tidligere omtalt kontrollaktiviteter som en del av internkontrollsystemet. Avdekking av avvik er til dels overlappende med kontrollaktivitetene i virksomhetene. Man kan ha faste og planlagte kontroller, eller gjennomføre stikkprøver. Ansattes rapportering på erfaringer fra den daglige driften og tjenesteytingen er også viktig for å fange opp avvik. Dette handler i mindre grad om kontrollaktiviteter, og foregår i større grad som en naturlig del ved tjenesteutøvelsen og den faglige kompetansen i tjenesten. Ofte har denne typen avvik et større volum ved innrapportering. I motsetning til kontrollaktiviteter, vil innmeldingen av slike avvik i større grad være avhengig av den enkeltes kunnskap om og kjennskap til kommunens rutiner, prosedyrer og faglig skjønn. God praksis for innmelding av avvik kan derfor i stor grad påvirkes gjennom opplæring.

Oppdagede eller innmeldte avvik må deretter følges opp og lukkes. Selve oppfølgingen vil avhenge av avviket. Noen avvik kan lukkes forholdsvis raskt, mens andre vil være vanskelige å anse som helt avsluttet. Det er vanlig at avvik meldes inn på laveste nivå og løftes videre og oppover i organisasjonen

[28] Kilde: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/forhandsdroftelser/

dersom det ikke er mulig å korrigere avviket på det innmeldte nivået. Det er også vanlig at man melder tilbake til melder om at avviket er mottatt og når et avvik er lukket. [29]

At internkontrollen skal følge opp risiko for at avvik kan forekomme innebærer at «kommunedirektøren må skaffe oversikt over områder i kommunen hvor det er fare for manglende etterlevelse av lover og forskrifter, og sette inn relevante forebyggende og risikoreduserende tiltak for å hindre og forebygge brudd på lover og forskrifter» [30]. Dette skal gjøres ut fra både et kortsiktig og et langsiktig perspektiv.

Det er også en intensjon om at avvik skal forebygges. Dette kan til dels tilskrives risikovurderingene som er gjennomført. Men det innebærer også at avvik som er innrapportert skal kunne brukes til læring og forbedring slik at rutiner og prosedyrer justeres på en måte som reduserer risikoen for at samme avvik forekommer igjen. [31]

Hamar kommune har sammen med øvrige kommuner i HIKT-samarbeidet valgt å jobbe med Normen som et utgangspunkt for gjennomgang av rutiner og prosedyrer i egen organisasjon. Normen inneholder et eget punkt som omhandler avvikshåndtering, samt flere punkter som omtaler hva et avvik konkret er i forhold til informasjonssikkerhet. I Normens punkt 5.8 fremgår det at virksomheter skal ha rutiner for å oppdage og å håndtere avvik. Denne avviksbehandlingen skal også dokumenteres.

Dokumentasjon av avviksbehandlingen betyr her at virksomheten innhenter fakta om hendelsesforløpet, som et grunnlag for etablering av korrigerende tiltak. Det fremgår videre at virksomheten skal evaluere tiltakene og eventuelt gjennomføre en ny risikovurdering dersom avvikene er alvorlige eller gjentar seg. Dersom avviksmeldingene inneholder personopplysninger eller opplysninger som har betydning for informasjonssikkerheten, skal avviksmeldingene sikres.

Hva som er et avvik vil avhenge av situasjonen, men Normen omtaler imidlertid noen eksempler:

- Virksomheten må etterleve kravene til konfidensialitet, integritet, tilgjengelighet og robusthet. Avvik fra disse kravene skal håndteres som avvik (punkt 3.2).
    - Konfidensialitet innebærer: at informasjonen ikke blir kjent for uvedkommende.
    - Integritet innebærer: at informasjonen ikke blir endret utilsiktet eller av uvedkommende.
    - Tilgjengelighet innebærer: at informasjonen er tilgjengelig for autoriserte ved behov.
    - Robusthet innebærer: at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser. [32]
- Brudd på taushetsplikten er å anse som et avvik (punkt 4.2.1).
- Misbruk av selvautentisering er å anse som et avvik (punkt 5.2.3).
- Urettmessig tilgang til systemer er å anse som et avvik (punkt 5.2.3).
- Urettmessig tilgang til personopplysninger er å anse som et avvik (punkt 5.2.3).

[29] Kilde: KS. Internkontroll. Side 100.

[30] Kilde: Prop. 81 L (2019-2020), kap. 4.3.1. https://www.regjeringen.no/no/dokumenter/prop.-81-l-20192020/id2697704/?ch=4

[31] Kilde: KS. Internkontroll. Side 99.

[32] Kilde: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/

- Avlesning og endring av opplysninger skal loggføres, og loggene skal analyseres. Dersom analyser av logger avdekker urettmessig avlesning eller endring av opplysninger, skal dette behandles som avvik (punkt 5.4.4.).
- Øvrige uønskede hendelser, som brudd på rutiner, personvern og informasjonssikkerhet, skal også anses som avvik.

I tillegg til at vi mener at det er naturlig at disse punktene forventes etterlevd av Hamar kommune, mener vi at det også er naturlig å forvente at kommunen bruker avvik til forbedring av gjeldende rutiner og prosedyrer. Det ligger til hensikten at internkontrollen også skal virke forebyggende. Det er også å forvente at kommunen sikrer opplæring av ansatte slik at man sikrer at avvik blir meldt inn. Dette gjelder både på informasjonssikkerhets- og personvernområdet, men også generelt for avviksmeldinger.

### Hamar kommunes rutiner

Vi har fått oversendt flere av Hamar kommunes rutiner for å ivareta informasjonssikkerhet, informasjonshåndtering og personvern. Seks av rutinene anses som relevante å kontrollere i forvaltningsrevisjonsprosjektet. Dette handler om

- Prosedyre for risikovurdering – personopplysninger (gyldig fra 7.6.2010, rev.frist 2.6.2014) – revisjon 1.1
- Prosedyre – når personopplysninger er kommet på avveie (gyldig fra 25.4.13, rev.frist 24.4.16) – revisjon 1.3
- Håndtering av dokumenter med sensitivt innhold – prosedyre (gyldig fra 27.9.13, rev.frist 26.9.2016) – revisjon 1.0
- Bruk av bærbart utstyr – prosedyre (gyldig fra 3.8.2015, rev.frist 2.8.2017) – revisjon 1.1
- Opplæringsskriv IKT-sikkerhet (gyldig fra 4.12.2015, rev.frist 3.12.2017) – revisjon 2.1
- Datavett regler (gyldig fra 7.1.2021, rev.frist 7.1.2022) – revisjon 1.8

I dette dokumentet stiller vi krav til at rutiner skal være oppdatert jamfør endringer i lov- og regelverk. Fem av de seks dokumentene har passert sine revisjonsfrister i henholdsvis 2014, 2016 og 2017. Ny personopplysningslov trådte i kraft i juli 2018, mens EUs personvernforordning trådte i kraft i mai 2018. eForvaltningsforskriften trådte i kraft i 2004, men har blitt endret flere ganger siden da, sist i oktober 2020.

Selv om flere av rutinene ikke er revidert etter oppdateringer i lovverket, er det likevel naturlig å kontrollere Hamar kommune for praktisering av disse rutinene siden det er disse som legges til grunn i kommunens organisasjon. De seks aktuelle rutinene har noen sammenfallende punkter, og vi vil liste opp de viktigste kravene kommunen stiller til egen organisasjon med henvisning til de aktuelle rutinene.

- Datavett regler:
    - Ansatte skal bruke sikre passord med kombinasjon av tall, bokstaver og tegn.
    - PC skal låses eller være slått av når man forlater arbeidsplassen.
    - Viktige dokumenter, minnepenner o.l. skal ikke ligge tilgjengelig for uvedkommende.
    - Minnepenner som man ikke kjenner innholdet av skal kontrolleres for datavirus før de tas i bruk.
    - Automatisk videresending til privat e-postkonto er ikke tillatt.
    - Taushetsbelagt informasjon, personopplysninger og virksomhetskritiske opplysninger skal ikke sendes over e-post.

        - Dersom man mottar e-post med slik informasjon, så skal den ikke videresendes eller besvares før sensitiv informasjon er fjernet.
    - Ansatte skal ikke søke etter personopplysninger som man ikke har tjenstlig behov for.
    - Dokumenter som inneholder sensitive personopplysninger skal være sikret mot uautorisert adgang, f.eks. ved bruk av rullerende passord eller at de er innelåst.
    - Dokumenter med sensitive personopplysninger som ikke lagres skal makuleres.
    - Ansatte plikter å melde avvik i forhold til gjeldende prosedyrer. [33]
- Bruk av bærbart utstyr:
    - Ansatt/bruker av utstyr skal melde til helpdesk (HIKT) så snart som mulig dersom utstyr blir stjålet/mistet eller mistanke om at maskinen er infisert med virus, spyware eller tilsvarende.
    - Ansatte skal ikke installere programmer på egenhånd uten at det først drøftes med kommunens sikkerhetsansvarlig.
- Håndtering av dokumenter med sensitivt innhold:
    - Utskrifter med sensitive personopplysninger og/eller med informasjon som er unntatt offentlighet skal hentes umiddelbart fra skriver.
    - Ved tap av dokumenter med sensitiv informasjon skal IKT-sikkerhetsansvarlig kontaktes.
- Når personopplysninger er kommet på avveie:
    - Prosedyren skal gjøres kjent for alle ansatte, dette ansvaret er lagt til resultatenhetsledere.
    - Alle ansatte skal melde alle tilfeller hvor personopplysninger er kommet på avveie.
        - Når et tilfelle meldes skal man iverksette strakstiltak for å redusere eller stoppe årsaken til hendelsen, ta kontakt med IKT-sikkerhetskoordinator for melding av avvik, varsle berørte individer om hendelsen og planer for å rette på forholdet, og informere de(n) berørte om sakens utfall dersom det er behov for det.
        - IKT-sikkerhetskoordinator skal vurdere om det er behov for å melde avviket til Datatilsynet, og foreta meldingen.
        - Det skal utarbeides en forebyggende plan, og for øvrig skal man følge vanlig avvikshåndtering med hensyn til behov for ytterligere tiltak for å redusere risiko for at det samme skjer igjen.
- Prosedyre for risikovurdering av personopplysninger:
    - Det skal gjennomføres risikovurderinger ved:
        - Innføring av nye systemer/behandlinger
        - Endringer i eksisterende løsninger som kan påvirke informasjonssikkerhet
        - Endringer i trusselbildet
    - Det skal benyttes en mal for rapport etter at man har utarbeidet risikovurdering. Denne inneholder nødvendige skjemaer for gjennomføring. Rapporten skal gi:
        - Oversikt over identifiserte trusler.
        - Angivelse av sannsynlighet for at en uønsket hendelse kan inntreffe.
        - Angivelse av konsekvenser av en uønsket hendelse.
        - Valgte skadereduserende og skadeforebyggende tiltak med ansvar og frist.
        - Resultat fra analyse av sikkerhetstiltakenes effekt i forhold til risiko.
        - Rapporten skal oversendes IKT-sikkerhetskoordinator og arkiveres i 5 år.

[33] Rutinen angir eksempler som a) ikke tilgang til fagsystem, b) feilført journal, c) personopplysninger på avveie, d) mistanke om passord på avveie.

- Opplæringskriv IKT sikkerhet
    - Ansatte skal melde avvik når noe er feil med programvare og ved feil i opplysningene i informasjonsbehandlingssystemene.
    - Opplysninger om tilganger og tilgangskontroll skal ikke formidles til andre, for eksempel koder og passord.
    - Dersom man må lagre data midlertidig på minnepinne, skal denne/disse oppbevares innelåst.
    - Alle nytilsatte skal gjennomgå sikkerhetsopplæring gjennom kommunens introduksjonsprogram.
    - Hver enkelt leder skal vurdere opplæringsbehov sammen med medarbeidere jevnlig.
    - Aktiviteter i IKT-systemene skal loggføres, og de skal gjennomgås jevnlig for å kontrollere for uautorisert virksomhet.
    - Hvert arbeidssted skal ha gjennomføre en sikkerhetsrevisjon for behandling av personopplysninger og bruk av informasjonssystemer årlig, ved bruk av et spørreskjema. Sikkerhetsledelsen ved arbeidsstedet/virksomheten skal også gjennomgå er sjekkliste for egenkontroll. Resultatene skal brukes av sikkerhetskoordinator som grunnlag for ledelsens gjennomgang.
    - Kommunedirektøren skal gjennomgå sikkerhetsarbeidet en gang i året.

## Punktvis oppsummering av revisjonskriteriene

Hamar kommune må:

1. kunne dokumentere at det er foretatt risiko- og vesentlighetsvurderinger knyttet til IT- og informasjonssikkerhet.
2. ha foretatt en vurdering av konsekvensene som brudd på personvern kan ha og en forhåndsdrøftelse av disse.
3. ha en informasjonssikkerhetsstrategi med målsettinger.
4. ha et tilfredsstillende system for informasjonssikkerhet og personvern, herunder
    - dokumenterte vurderinger av hvilke rutiner og prosedyrer som er nødvendige,
    - utarbeidelse av nødvendige rutiner og prosedyrer, og
    - sørge for at rutinene og prosedyrene blir vedlikeholdt/oppdatert ved behov.
5. ha rutiner for autorisering, endring og avslutning av tilganger.
6. ha retningslinjer for privat bruk av informasjonssystemer og utstyr.
7. ha nødvendige rutiner og prosedyrer som sikrer tilfredsstillende håndtering av personopplysninger, og som oppdateres ved behov.
8. ha et avvikssystem som tilfredsstiller at avvik avdekkes, behandles, lukkes og som bidrar til avvik blir forebygget, herunder:
    - jevnlig gjennomgang av avvik for å vurdere forbedringspotensial.
9. sikre avviksmeldinger som inneholder personopplysninger eller har betydning for informasjonssikkerheten.
10. ha identifisert hvilke personopplysninger de har.
11. ha fastsatt formål for behandlingen av personopplysninger.
12. føre protokoller over alle behandlingsaktiviteter.

13. på en kort og forståelig måte gi informasjon om hvordan de behandler personopplysningene.
14. ha et personvernombud og opplyse for ansatte og andre hvem personvernombudet er.
15. ha databehandleravtaler.
16. ha tiltak som sørger for tilstrekkelig kompetanse i organisasjonen vedrørende informasjonssikkerhet og personvern.
17. følge egne rutiner for informasjonssikkerhet og personvern.

# Referanser

Datatilsynet. Virksomhetenes plikter. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

Datatilsynet. Hva er en behandlingsansvarlig? https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/behandlingsansvarlig-og-databehandler/hva-er-en-behandlingsansvarlig/

Digitaliseringsdirektoratet. Internkontroll i praksis - informasjonssikkerhet. Grunnleggende begreper. https://internkontroll-infosikkerhet.difi.no/sites/sikkerhet/files/grunnleggende_begreper_-_internkontroll_informasjonssikkerhet.pdf

Digitaliseringsdirektoratet. Internkontroll i praksis – informasjonssikkerhet. Grunnleggende innføring. https://internkontroll-infosikkerhet.difi.no/sites/sikkerhet/files/grunnleggende_innforing_-_internkontroll_informasjonssikkerhet.pdf

Digitaliseringsdirektoratet. Internkontroll i praksis – informasjonssikkerhet. For toppleder. https://internkontroll-infosikkerhet.difi.no/sites/sikkerhet/files/for_toppledere_-_internkontroll_informasjonssikkerhet.pdf

Digitaliseringsdirektoratet. Hva sier ISO/IEC 27001? https://internkontroll-infosikkerhet.difi.no/hva-sier-isoiec-27001

Digitaliseringsdirektoratet. Regelverkskrav. https://internkontroll-infosikkerhet.difi.no/regelverkskrav

Digitaliseringsrundskrivet 2022. https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2895185/

Direktoratet for e-helse. 2020. Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren. https://www.ehelse.no/normen

eForvaltningsforskriften med noter: https://www.regjeringen.no/contentassets/be9697d7e68041e29ffca576c331b4b0/efvf_del3.pdf

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften). https://lovdata.no/dokument/SF/forskrift/2004-06-25-988

Kommunal- og moderniseringsdepartementet. 2021. Veileder om kommunelovens internkontrollbestemmelser. https://www.regjeringen.no/no/dokumenter/internkontroll-i-kommunesektoren/id2876831/

KS. 2020. Orden i eget hus. Kommunedirektørens internkontroll. En praktisk veileder. https://www.ks.no/globalassets/fagomrader/lokaldemokrati/internkontroll/Kommunedirektorens-internkontroll-veileder-F41-web.pdf

Lov om kommuner og fylkeskommuner (kommuneloven). https://lovdata.no/dokument/NL/lov/2018-06-22-83

Nasjonal sikkerhetsmyndighet. 2021. Sikkerhetskultur. https://nsm.no/fagomrader/sikkerhetsstyring/sikkerhetskultur/

NorSIS. 2017. Sikkerhetskultur. https://norsis.no/sikkerhetskultur/

NorSIS. 2021. Trusler og trender. https://norsis.no/download/20115/

GDPR (personvernforordningen). 2016. Artikkel 4. https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_4#gdpr/ARTIKKEL_4

Prop. 81 L (2019-2020). Endringer av internkontrollregler i sektorlovgivningen (tilpasning til ny kommunelov). https://www.regjeringen.no/no/dokumenter/prop.-81-l-20192020/id2697704/?ch=4

Standard Norge. 2017. NS-EN ISO/IEC 27001: 2017.