



RAPPORT NR. 13-2026

# **PERSONVERN OG INFORMASJONSSIKKERHET**

## **NANNESTAD KOMMUNE**

FORVALTNINGSREVISJON

OKTOBER 2026

# INNHold

|                                                                                            |           |
|--------------------------------------------------------------------------------------------|-----------|
| <b>SAMMENDRAG .....</b>                                                                    | <b>1</b>  |
| <b>1 INNLEDNING .....</b>                                                                  | <b>3</b>  |
| 1.1 Bakgrunn for prosjektet.....                                                           | 3         |
| 1.2 Formål og problemstillinger.....                                                       | 3         |
| 1.3 Metode.....                                                                            | 4         |
| 1.3.1 Generelt.....                                                                        | 4         |
| 1.3.2 Dokumentanalyse.....                                                                 | 4         |
| 1.3.3 Intervju.....                                                                        | 4         |
| 1.3.4 Verifiseringsprosesser.....                                                          | 4         |
| 1.4 Kommunedirektørens uttalelse.....                                                      | 5         |
| 1.5 Revisjonskriterier .....                                                               | 5         |
| 1.6 Organisering av arbeidet med personvern og informasjonssikkerhet i Nannestad kommune . | 5         |
| 1.7 Begrepsforklaringer.....                                                               | 7         |
| <b>2 RISIKOVURDERINGER .....</b>                                                           | <b>9</b>  |
| 2.1 Problemstilling og revisjonskriterier.....                                             | 9         |
| 2.2 Risikovurderinger .....                                                                | 9         |
| 2.3 Vurderinger av personvernkonsekvenser (DPIA) .....                                     | 12        |
| 2.4 Revisjonens vurdering .....                                                            | 13        |
| <b>3 SIKRING AV PERSONOPPLYSNINGER.....</b>                                                | <b>15</b> |
| 3.1 Problemstilling og revisjonskriterier.....                                             | 15        |
| 3.2 Internkontroll med informasjonssikkerhet og personvern .....                           | 16        |
| 3.2.1 Grunnleggende krav på området .....                                                  | 16        |
| 3.2.2 Styringsdokumenter.....                                                              | 16        |
| 3.2.3 Roller og ansvar.....                                                                | 17        |
| 3.3 Protokoll over personopplysninger (behandlingsprotokoll) .....                         | 19        |
| 3.4 Kontroll på identiteter og tilganger.....                                              | 20        |

|          |                                                                                                      |           |
|----------|------------------------------------------------------------------------------------------------------|-----------|
| 3.5      | Sikkerhetsovervåkning .....                                                                          | 21        |
| 3.6      | Inntrengingstester .....                                                                             | 21        |
| 3.7      | Databehandleravtaler .....                                                                           | 21        |
| 3.8      | Opplæring i personvern .....                                                                         | 22        |
| 3.9      | Revisjonens vurdering .....                                                                          | 23        |
| <b>4</b> | <b>KONKLUSJON OG ANBEFALINGER.....</b>                                                               | <b>25</b> |
|          | <b>LITTERATUR- OG KILDELISTE .....</b>                                                               | <b>26</b> |
|          | <b>VEDLEGG 1 REVISJONSKRITERIER .....</b>                                                            | <b>28</b> |
|          | Revisjonskriterier og kilder .....                                                                   | 28        |
|          | Risikovurderinger .....                                                                              | 28        |
|          | Generelt om internkontroll og risikovurderinger knyttet til informasjonssikkerhet og personvern..... | 28        |
|          | Risikoreduserende tiltak og restrisiko.....                                                          | 29        |
|          | Vurdering av personvernkonsekvenser (DPIA) .....                                                     | 29        |
|          | Personopplysninger .....                                                                             | 30        |
|          | Generelt om krav etter personopplysningsloven .....                                                  | 30        |
|          | Internkontroll med personvern og informasjonssikkerhet.....                                          | 31        |
|          | Behandlingsprotokoll.....                                                                            | 32        |
|          | Kontroll på identiteter og tilganger.....                                                            | 32        |
|          | Sikkerhetsovervåkning .....                                                                          | 33        |
|          | Inntrengingstester .....                                                                             | 33        |
|          | Databehandleravtaler.....                                                                            | 33        |
|          | Opplæring i informasjonssikkerhet .....                                                              | 34        |

## Figurer

|                                                                                               |           |
|-----------------------------------------------------------------------------------------------|-----------|
| <b>Figur 1 Administrativ organisering i Nannestad kommune .....</b>                           | <b>6</b>  |
| <b>Figur 2 Styringsmodellen i DGI.....</b>                                                    | <b>7</b>  |
| <b>Figur 3 Illustrasjon av oversikten over risikovurderinger i kvalitetssystemet.....</b>     | <b>10</b> |
| <b>Figur 4 Illustrasjon av hvordan et risikoscenario registreres i kvalitetssystemet.....</b> | <b>11</b> |

## SAMMENDRAG

Romerike revisjon har gjennomført en forvaltningsrevisjon av personvern og informasjonssikkerhet i Nannestad kommune. Prosjektet ble bestilt av kontrollutvalget i Nannestad kommune 23.10.2025 i sak 37/25. Formålet med forvaltningsrevisjonen har vært å avdekke eventuelle svakheter i informasjonssikkerheten og ivaretagelsen av personvern i Nannestad kommune, slik at feil kan rettes og systemer kan gjøres sikrere.

### Hovedfunn

1. Kommunen har ikke tilstrekkelig internkontroll med informasjonssikkerhet og personvern, blant annet ved at roller og ansvar ikke er tilstrekkelig avklart og at det ikke gjennomføres ledelsens gjennomgang av informasjonssikkerhet.
2. Kommunen har rutiner og prosedyrer som sikrer at det gjennomføres vurderinger av personvernkonsekvenser, men vurderingene er ikke tilstrekkelig dokumentert.
3. Kommunens protokoll over behandling av personopplysninger er ikke oppdatert.
4. Kommunen har ikke et tilstrekkelig systematisert opplegg for opplæring i informasjonssikkerhet og personvern.

Kommunen har etablert et styringssystem for informasjonssikkerhet blant annet gjennom arbeidet som gjennomføres i DGI-samarbeidet. Undersøkelsen viser imidlertid at roller og ansvar ikke er tilstrekkelig avklart på flere områder. Det gjennomføres ikke ledelsens gjennomgang av informasjonssikkerhet i kommunedirektørens ledergruppe årlig, noe som er anbefalt for å sikre en systematisk oppfølging av området.

Kommunen gjennomfører risikovurderinger av informasjonssikkerhet og personvern, og disse følges langt på vei opp. Kommunen har imidlertid et forbedringspotensial knyttet til dokumentasjonen av vurderinger av personvernkonsekvenser som gjennomføres, særlig knyttet til innhenting av vurderinger, informasjon om deltakere og tidspunkt for gjennomgangene samt aksept av restrisiko.

Det er opprettet en protokoll over behandlinger av personopplysninger, men denne er ikke ferdigstilt eller oppdatert etter at den ble etablert. Det er uklart hvem som har ansvar for å følge opp protokollen.

Kommunen har etter revisjonens syn ikke tilstrekkelig systematisert obligatorisk opplæring av ledere og ansatte i informasjonssikkerhet og personvern. Kommunen har noen opplæringstiltak, blant annet knyttet til nyansatte, men ut over dette er det revisjonens inntrykk at det er opp til den enkelte ansatte og den enkelte leder å holde seg oppdatert om informasjonssikkerhet og personvern.

Basert på det som kommer frem i undersøkelsen anbefaler revisjonen at kommunedirektør:

1. sørger for tilstrekkelig internkontroll med informasjonssikkerhet i Nannestad kommune, herunder
  - a. å gjennomføre ledelsens gjennomgang av informasjonssikkerhet årlig
  - b. å sikre en tydelig rolle- og ansvarsfordeling
2. sikrer at vurderinger av personvernkonsekvenser dokumenteres i tilstrekkelig grad
3. sikrer at kommunens protokoll over behandlinger av personopplysninger oppdateres og følges opp jevnlig
4. sørger for systematisk opplæring i personvern og informasjonssikkerhet

# 1 INNLEDNING

## 1.1 Bakgrunn for prosjektet

Kontrollutvalget i Nannestad kommune bestilte i møte 23.10.2025 (sak 37/25) et forvaltningsrevisjonsprosjekt av IT-sikkerhet og personvern, og ba revisjonen om å legge frem en prosjektplan.

Den økende digitale kompleksiteten i samfunnet fører til store utfordringer i kommunesektoren, hvor det er mange små enheter som har ansvar for viktige systemer og tjenester. I tillegg har kommunene ofte problemer med å skaffe tilstrekkelig kompetanse på IKT-sikkerhet (NOU 2015:13).

Solid IKT-sikkerhet og et tilstrekkelig personvern i kommunene er avgjørende for å beskytte innbyggernes personopplysninger og sikre viktige samfunnsfunksjoner. Innbrudd i en kommunes IT-systemer kan ha store konsekvenser. Østre Toten kommune ble utsatt for et dataangrep i 2021 hvor alle sikkerhetskopier i kommunen ble slettet og alle data ble kryptert. Dette gjorde at ingen av de 1300 ansatte i kommunen kunne bruke datasystemene og at sensitive personopplysninger, blant annet fra helse- og omsorgstjenestene, NAV og barnevernstjenestene, kom på avveie (Datatilsynet 2022). I mai 2026 ble det avdekket et alvorlig dataangrep i Lørenskog kommune som førte til at svært store mengder sensitive data havnet på det mørke nettet. NRK har funnet 264 enkeltvedtak fra barnevernet, 780 loggførte samtaler mellom kommunens psykologiske hjelpetjeneste og navngitte innbyggere, samt 1400 saker fra psykologhelsetjenesten for barn og unge med fullt navn og detaljerte journaler blant dokumentene som ligger på det mørke nettet.

## 1.2 Formål og problemstillinger

Formålet med undersøkelsen er å avdekke eventuelle svakheter i informasjonssikkerheten og ivaretagelsen av personvern i Nannestad kommune, slik at feil kan rettes og systemer kan gjøres sikrere.

Undersøkelsen vil besvare følgende problemstillinger:

1. Gjennomføres det nødvendige risikovurderinger knyttet til informasjonssikkerhet og personvern og hvordan følges risikovurderingene opp?
2. Har kommunen sørget for at personopplysninger som lagres i kommunens IT-systemer er sikret i tilstrekkelig grad?

Når det gjelder problemstilling 1 så har ikke revisjonen forutsetninger for å vurdere *hvilke* risikovurderinger som er nødvendige å gjennomføre. Revisjonen vil derfor undersøke om og når det gjennomføres risikovurderinger om informasjonssikkerhet og personvern og om disse blir gjennomført på en systematisk måte og i henhold til etablerte rutiner.

Når det gjelder problemstilling 2 er det viktig å presisere at revisjonen ikke har revidert den tekniske sikkerheten i IT-systemene. Vi har primært undersøkt styring, internkontroll, dokumentasjon og prosesser.

## 1.3 Metode

### 1.3.1 Generelt

Undersøkelsen er gjennomført i henhold til RSK 001 - Standard for forvaltningsrevisjon som er fastsatt av styret i NKRF - Kontroll og revisjon i kommunene. Standarden definerer hva som er god revisjonsskikk innen kommunal forvaltningsrevisjon. Arbeidet er kvalitetssikret i henhold til Romerike revisjon IKS sine interne rutiner.

### 1.3.2 Dokumentanalyse

Revisjonen har i dokumentbestilling bedt administrasjonen oversende dokumenter knyttet til hver av de to problemstillingene. Slik problemstillingene er formulert, vil disse i utgangspunktet kunne la seg besvare gjennom en dokumentanalyse. Dokumentasjonen er i denne sammenheng revisjonsbevis med både høy pålitelighet og gyldighet.

Revisjonen har etterspurt og mottatt styrende dokumenter som strategier, prosedyrer, retningslinjer og maler som omhandler informasjonssikkerhet og personvern. Videre har revisjonen bedt om et utvalg gjennomførte risikovurderinger og vurderinger av personvernkonsekvenser (DPIA). Kriterier for utvalget er at de er gjennomført relativt nylig (de siste få årene) og at de ulike tjenesteområdene i kommunen er representert. Revisjonen har mottatt syv risikovurderinger og fire DPIA.

### 1.3.3 Intervju

For å supplere dokumentgjennomgangen er det gjennomført intervjuer med ansatte i kommunen med roller og ansvar knyttet til temaene som undersøkes. Formålet med intervjuene har vært å få en bedre forståelse for hvordan kommunen jobber med personvern og informasjonssikkerhet, få oppklaringer i tilfeller hvor dokumentasjon mangler og få informasjon som ikke uten videre kan leses ut fra dokumentene. Dette bidrar til å styrke både pålitelighet og gyldighet i datagrunnlaget.

Revisjonen har intervjuet følgende ansatte i Nannestad kommune:

- Fagansvarlig IKT-sikkerhet
- Fagansvarlig digitalisering
- Kommunalsjef HR og digitalisering
- Kommunalsjef helse og mestring
- Kommunalsjef samfunn, kultur og inkludering
- Konstituert kommunalsjef oppvekst

Revisjonen har i tillegg hatt et felles intervju med vikarierende og faste personvernombud, samt sikkerhetssjefen i DGI.

Revisjonen har ikke gjennomført konkrete kontroller av tilgangsstyringen. Vi har sett på prosedyrer på området, samt spurt om hvordan disse etterleves i intervju. Dette er en svakhet i datagrunnlaget som vi tar høyde for i vurderingen.

### 1.3.4 Verifiseringsprosesser

Oppsummering av intervju er sendt til de som er intervjuet for verifisering, og informasjon fra de verifiserte intervjureferatene er benyttet i rapporten.

Rapporten ble sendt administrasjonen i sin helhet til gjennomgang og uttalelse 21.8.2026. Revisjonen har mottatt tilbakemeldinger på faktagrunnlaget i på epost mottatt hhv. 4.9.2026 og 23.9.2026. Vi har gjennomgått tilbakemeldingene og gjort nødvendige justeringer i faktagrunnlaget på bakgrunn av disse.

Revisjonen mener gode verifiseringsprosesser knyttet til muntlige fremkommet data, og av rapporten i sin helhet, er viktig for å sikre gyldighet og pålitelighet i undersøkelsens datagrunnlag.

#### **1.4 Kommunedirektørens uttalelse**

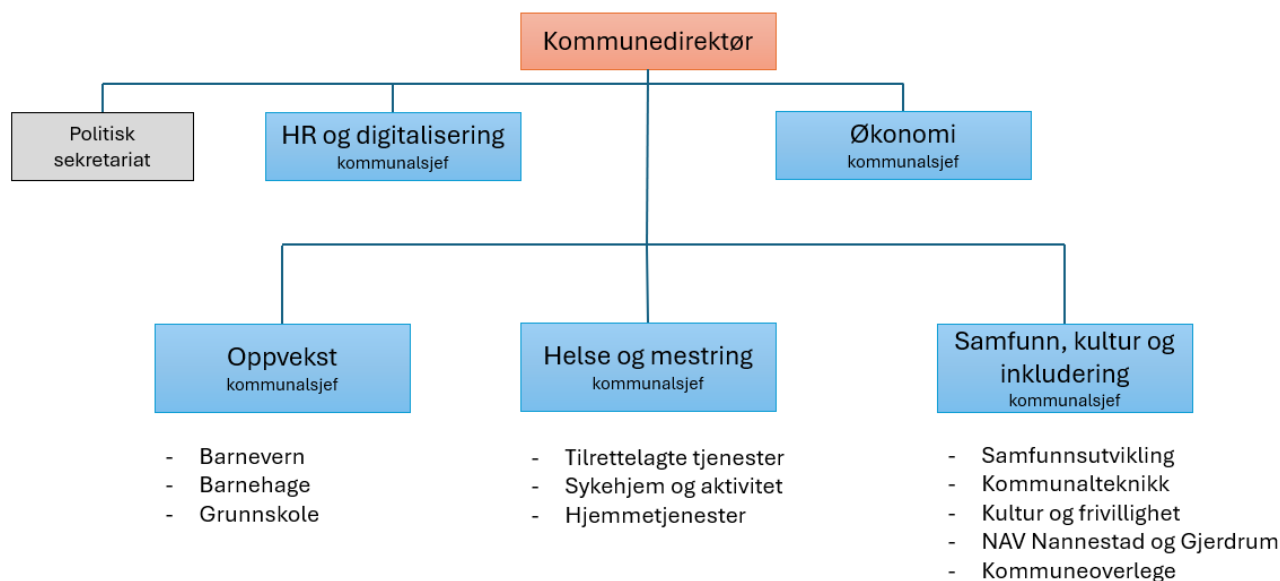
Kommunedirektøren skriver i e-post mottatt 29.9.2026 at han ikke har noen andre kommentarer til rapporten ut over tilbakemeldingene på faktagrunnlaget nevnt over. Vi har derfor ikke lagt denne e-posten som eget vedlegg til denne rapporten, siden den i praksis ikke inneholder noen uttalelse til rapportens funn og anbefalinger.

#### **1.5 Revisjonskriterier**

Revisjonskriterier er de krav og forventninger som kommunen vurderes opp mot. Kriteriene utledes fra lover og forskrifter, kommunestyrets vedtak og hva som anses som god forvaltningsskikk og faglig anerkjente normer på området. I dette prosjektet er revisjonskriteriene blant annet hentet fra personopplysningsloven, kommuneloven og eForvaltningsforskriften. Kriteriene er nærmere presentert innledningsvis i kapittel 2 og 3, og i vedlegg 2 i rapporten.

#### **1.6 Organisering av arbeidet med personvern og informasjonssikkerhet i Nannestad kommune**

Nannestad kommune gjennomgikk en omorganisering i mai 2025. Figuren under viser den administrative organiseringen i Nannestad kommune per 1. oktober 2025.

**Figur 1 Administrativ organisering i Nannestad kommune**

Kilde: Basert på kommunens organisasjonskart pr. 1.10.2025<sup>1</sup>.

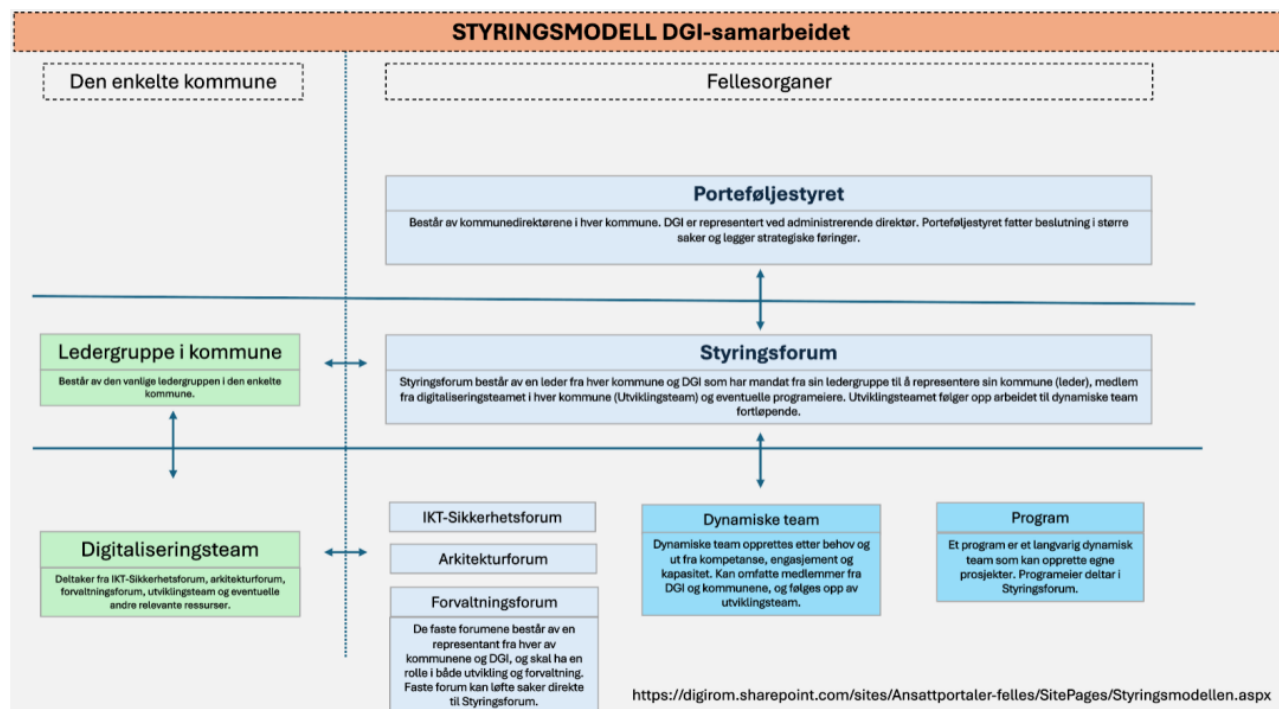
Nannestad kommune er en del av IKT-samarbeidet Digitale Gardemoen (DGI). DGI er organisert som et kommunalt oppgavefellesskap. Representantskapet er DGIs øverste organ og består av ordførerne i de fem eierkommunene. Styret består av kommunedirektørene fra eierkommunene, samt en ansattvalgt representant.<sup>2</sup>

I mars 2025 ble det vedtatt en ny styringsmodell i DGI-samarbeidet, fremstilt i figur 2 under. Hver kommune i DGI-samarbeidet har et digitaliseringsteam som blant spiller inn digitale initiativ fra kommunene til IKT-sikkerhetsforum i DGIs styringsmodell. I Nannestad kommune ledes digitaliseringsteamet av fagleder digitalisering og hvert kommunalområde bidrar med ressurser inn i digitaliseringsteamet. Kommunen har videre en fagansvarlig IKT-sikkerhet som sitter i IKT-sikkerhetsforum i DGI-samarbeidet. Kommunedirektørene deltar i porteføljestyret.

<sup>1</sup> Hentet 30.9.2026 fra <https://www.nannestad.kommune.no/tjenester/politikk-og-planer/administrativ-organisering/>

<sup>2</sup> Hentet 30.9.2026 fra <https://www.dgi.no/om-dgi/>

Figur 2 Styringsmodellen i DGI



Kilde: DGI-samarbeidets ansattportal.

## 1.7 Begrepsforklaringer

**Informasjonssikkerhet og IKT-sikkerhet:** Informasjonssikkerhet er krav til pålitelighet og sikkerhet knyttet til (sensitiv) informasjon (NAOB 2026). Informasjonssikkerhet handler om å sikre at informasjon i alle former ikke blir kjent for uvedkommende, ikke blir endret utilsiktet eller av uvedkommende og å sikre at informasjonen er tilgjengelig ved behov (Digdir 2026). IKT-sikkerhet (informasjons- og kommunikasjonsteknologi) handler om å beskytte IKT-systemer og informasjonen i disse. Med andre ord handler IKT-sikkerhet om beskyttelse av det som er sårbart fordi det er koblet til eller er avhengig av informasjons- og kommunikasjonsteknologi (Meld. St. 38 2016-2017, s. 14). I denne rapporten benyttes hovedsakelig begrepet informasjonssikkerhet. I noen tilfeller blir imidlertid begrepet IKT-sikkerhet brukt, for eksempel i stillingstitler eller i tilfeller hvor kilden det vises til bruker dette begrepet.

**Styringssystem:** En kommunes styringssystem er en systematisk tilnærming til de sentrale aktivitetene for styring og kontroll i en virksomhet. I denne rapporten blir styringssystem for informasjonssikkerhet brukt synonymt med begrepene internkontroll og styring av informasjonssikkerhet og ledelsessystem, jf. Digdir sin veileder *Internkontroll i praksis – Informasjonssikkerhet*.

**Personopplysninger:** I personvernforordningen blir begrepet personopplysninger definert som enhver opplysning om en identifisert eller identifiserbar fysisk person. En identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres ved hjelp av en identifikator. Identifikatorer

kan f.eks. være et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet (personvernforordningen artikkel 4 nr. 1).

**Behandling av personopplysninger:** Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke. Dette kan for eksempel være innsamling, registrering, lagring, utlevering og sletting av personopplysninger (personvernforordningen artikkel 4 nr. 2).

**Behandlingsansvarlig:** En behandlingsansvarlig er den virksomheten eller enheten som bestemmer formålet med, og midlene for, behandlingen av personopplysninger, jf. personvernforordningen artikkel 4 nr. 7.

**Databehandler:** Databehandler er en aktør som behandler personopplysninger på vegne av den behandlingsansvarlige. Dette innebærer at databehandleren ikke bestemmer formål eller andre vesentlige sider ved behandlingen, men følger instruksjoner fra den behandlingsansvarlige. Eksempler på databehandlere i en kommune er IT-leverandører, systemdriftsleverandører og leverandører av skytjenester som behandler data på vegne av kommunen.

**Behandlingsprotokoll:** En behandlingsprotokoll er en oversikt, som virksomheten er lovpålagt å føre, over sine behandlinger av personopplysninger, jf. personvernforordningen artikkel 30. Protokollen skal blant annet beskrive hvilke personopplysninger som behandles, til hvilke formål, med hvilket rettslig grunnlag, hvem som har tilgang til opplysningene, hvor lenge de lagres og hvordan sikkerheten ved behandlingen ivaretas.

**DPIA** (Data Protection Impact Assessment): DPIA er en vurdering av personvernkonsekvenser. Dette er en plikt virksomheter har etter personvernregelverket til å vurdere konsekvensene for personvernet når nye løsninger tas i bruk. Vurderingen skal bidra til å håndtere de risikoene behandling av personopplysninger har for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastlegge risikoreduserende tiltak (Datatilsynet 2026b).

## 2 RISIKOVURDERINGER

### 2.1 Problemstilling og revisjonskriterier

Økt digitalisering i offentlig sektor fører med seg økt risiko for datainnbrudd og hendelser som kan få store konsekvenser for kommunenes tjensteproduksjon og innbyggernes personvern. Konsekvensene kan blant annet være driftsavbrudd, tap av kritisk informasjon, økonomiske tap og at personopplysninger kommer på avveie (KS 2025). For å få oversikt over mulige uønskede hendelser og bidra til at sikkerhets- og personvernarbeidet rettes mot områdene med høyest risiko er det viktig at kommunene identifiserer, analyserer og evaluerer risiko (Digdir 2025, KS 2025).

For problemstilling 1 utledes følgende krav og forventninger til kommunen:

| Problemstilling 1                                                                                                                       | Krav og forventninger til kommunen                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gjennomføres det nødvendige risikovurderinger knyttet til informasjonssikkerhet og personvern og hvordan følges risikovurderingene opp? | <p>Kommunen skal ha rutiner og praksis som sikrer at:</p> <ul style="list-style-type: none"><li>→ det gjennomføres risikovurderinger knyttet til informasjonssikkerhet og personvern</li><li>→ risikoreduserende tiltak etableres, gjennomføres og følges opp</li><li>→ restrisiko aksepteres etter risikoanalyser og risikoreduserende tiltak</li><li>→ det gjennomføres vurderinger av personvernkonsekvenser (DPIA)</li></ul> |

### 2.2 Risikovurderinger

Revisjonen har mottatt en prosedyre for gjennomføring av risikovurderinger og vurderinger av personvernkonsekvenser som er felles for kommunene i DGI-samarbeidet. Hensikten med prosedyren er ifølge dokumentet å sikre at alle digitale løsninger og prosesser i kommunefellesskapet vurderes med hensyn til informasjonssikkerhet og personvern. Videre er hensikten med prosedyren å bidra til systematisk gjennomføring av risikovurderinger og vurderinger av personvernkonsekvenser for digitale verktøy, med tydelig ansvarsfordeling og involvering av relevante roller. Prosedyren beskriver ansvar og myndighet, definisjoner av roller som er involvert i risikovurderinger samt en oversikt over hvordan risikovurderinger og vurderinger av personvernkonsekvenser skal gjennomføres. Prosedyren gjelder både for risikovurderinger som gjennomføres i DGI-samarbeidet og i kommunene. Prosedyren beskriver hvem som skal delta i risikovurderinger, samt hvem som kan delta dersom relevant (DGI-kommunene 2025).

Ifølge prosedyren skal tiltak identifiseres og planlegges. Når risikovurderingen er ferdig sendes den til systemeier for aksept eller avvisning av risiko. Systemeier er ofte en leder i kommunen, for eksempel en enhetsleder eller en kommunalsjef. Det er ifølge prosedyren systemeier som har ansvar for å følge opp de risikoreduserende tiltakene som er identifisert og planlagt (DGI-kommunene 2025). Beskrivelsene fagansvarlig IKT-sikkerhet, fagleder digitalisering og kommunalsjefene for de ulike tjenesteområdene gir i intervjuene av hvordan risikovurderinger gjennomføres, er i tråd med prosedyren. Revisjonen har også i intervju blitt vist hvordan risikovurderingene gjennomføres i kommunens kvalitetssystem.

Figuren under viser hvordan gjennomførte og pågående risikovurderinger om informasjonssikkerhet ser ut i verktøyet for risikovurderinger i kommunens kvalitetssystem. For hver risikovurdering går det frem hvor mange initielle risikoelementer som er identifisert, i tillegg til risikoelementer som gjenstår etter gjennomførte tiltak. Oversikten viser også om restrisiko er akseptert av systemeier.

**Figur 3 Illustrasjon av oversikten over risikovurderinger i kvalitetssystemet**

| ID   | Vurdert    | Initiell | Initiell | Beskrivelse | Område              | Status tiltak          | Endelig | Endelig | Akseptert        |
|------|------------|----------|----------|-------------|---------------------|------------------------|---------|---------|------------------|
| 1919 | 15.01.2026 | 20       |          |             | Kommunedire...      | Under gjennomføring    | 12      |         | ✗ Ikke akseptert |
| 1967 | 27.11.2025 |          |          |             | HR og digitalis...  | Tiltak ikke registrert |         |         | ✗ Ikke akseptert |
| 1870 | 17.11.2025 | 6        |          |             | Tilrettelagte tj... | Tiltak utført          | 6       |         | ✓ Akseptert      |
| 1906 | 13.11.2025 | 4        |          |             | Kommunaltek...      | Under gjennomføring    | 4       |         | ✓ Akseptert      |
| 1972 | 06.11.2025 | 9        |          |             | Service, drift o... | Under gjennomføring    | 9       |         | ✗ Ikke akseptert |
| 1924 | 03.09.2025 | 1        |          |             | Service, drift o... | Under gjennomføring    | 1       |         | ✗ Ikke akseptert |
| 1857 | 07.08.2025 | 8        |          |             | HR og digitalis...  | Tiltak utført          | 6       |         | ✓ Akseptert      |
| 1744 | 31.10.2024 | 9        |          |             | Service, drift o... | Under gjennomføring    | 6       |         | ✓ Akseptert      |
| 1617 | 25.06.2024 | 8        |          |             | HR og digitalis...  | Tiltak utført          | 8       |         | ✓ Akseptert      |
| 1513 | 31.01.2024 | 6        |          |             | Kommunaltek...      | Under gjennomføring    | 6       |         | ✗ Ikke akseptert |

Kilde: Skjermtutklipp fra kommunens kvalitetssystem tatt 17.2.2026.

Fagansvarlig digitalisering og fagansvarlig IKT-sikkerhet forteller i intervju at risikovurderinger skal gjennomføres når det skal innføres nye digitale systemer i kommunen. Eksempelvis forteller konstituert kommunalsjef for oppvekst i intervju at risikoanalyser gjennomføres når det skal innføres nye fagsystemer, og at hun har deltatt i disse på skoleområdet i rollen som virksomhetsleder.

Revisjonen har mottatt dokumentasjon på seks risikovurderinger av informasjonssikkerhet og personvern som er gjennomført innenfor de ulike tjenesteområdene i Nannestad kommune, samt kommunens siste gjennomførte helhetlige risiko- og sårbarhetsvurdering (ROS). Konstituert kommunalsjef for oppvekst forteller i intervju at DGI har deltatt i risikovurderinger ved behov, men at intensjonen er at kommunen skal være i stand til å gjennomføre sine egne risikovurderinger selv.

De seks risikovurderingene revisjonen har mottatt er knyttet til innføringen av ulike digitale systemer i skole, psykisk helse, kommunalteknikk og administrasjon. Gjennomgangen av de seks risikovurderingene viser at det i risikovurderingene blir identifisert risikoreduserende tiltak og at gjennomføringen av disse er delegert til ulike saksbehandlere og med frister for gjennomføringen. I risikovurderingene oppgis det videre hvorvidt tiltakene er gjennomført i tillegg til en vurdering av tiltakets effekt. I noen av risikovurderingene revisjonen har gjennomgått oppgis det at tiltakene er gjennomført, mens i andre vurderinger står det at tiltakene er under gjennomføring. I to av

risikoanalysene står tiltak markert med «under gjennomføring» selv om fristen for gjennomføring er passert og aksept av restrisiko for risikovurderingen er akseptert. Fagansvarlig IKT-sikkerhet forteller i intervju at hun deltar i alle risikovurderinger som omhandler informasjonssikkerhet og personvern. Risikovurderingene gjennomføres ved at hun oppretter risikovurderingen i kvalitetssystemet, så fasiliteter hun gjennomføringen av analysen. Det gjennomgås ulike risikoscenarioer, som blant annet er hentet fra KS. Hun forteller at hver risiko bli markert med grønt, gult og rødt avhengig av vurderingene av sannsynlighet og konsekvenser for identifisert risiko (se figur 4 under for hvordan et risikoscenario blir registrert i kvalitetssystemet). Alle risikomomenter som markeres med gult og rødt skal man sette tiltak på. Hvert tiltak blir tildelt en ansvarlig saksbehandler som jobber i den aktuelle tjenesten, og det settes en frist for når tiltaket skal være gjennomført. Et eksempel på tiltak kan være at det skal lages en ny prosedyre. Når tiltaket er gjennomført blir det sendt til virksomhetsleder for godkjenning. Virksomhetsleder godkjenner tiltaket. Når alle tiltak knyttet til risikovurderingene er gjennomført er det virksomhetsleder som aksepterer restrisiko. Dersom det dukker opp nye momenter, skal risikovurderingen revideres.

**Figur 4 Illustrasjon av hvordan et risikoscenario registreres i kvalitetssystemet**

Risikovurdering

BESKRIVELSE AV VURDERING

Tjenesteadministrator oppretter roller med tilgang til mer eller mindre informasjon enn det er tjenstlig behov for. Kan føre til informasjon på avveie eller dårligere tjenestetilbud

Risiko Mulighet

| Initiell risiko                                                                          | Endelig risiko                                                                           |
|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| <b>INITIELL SANNSYNLIGHET</b><br>Mindre sannsynlig - hendelsen kan inr ▼                 | <b>ENDELIG SANNSYNLIGHET</b><br>Mindre sannsynlig - hendelsen kan inr ▼                  |
| <b>LIV OG HELSE</b><br>2 - Begrenset (Liten/små skader, konsi) ▼ 4                       | <b>LIV OG HELSE</b><br>2 - Begrenset (Liten/små skader, konsi) ▼ 4                       |
| <b>YTRE MILJØ</b><br>1 - Ubetydelig (Ingen miljøskade eller) ▼ 2                         | <b>YTRE MILJØ</b><br>1 - Ubetydelig (Ingen miljøskade eller) ▼ 2                         |
| <b>ØKONOMI</b><br>1 - Ubetydelig (Små eller ingen skade) ▼ 2                             | <b>ØKONOMI</b><br>1 - Ubetydelig (Små eller ingen skade) ▼ 2                             |
| <b>DRIFT OG KONTINUITET</b><br>1 - Ubetydelig (Mindre forstyrrelser i d) ▼ 2             | <b>DRIFT OG KONTINUITET</b><br>1 - Ubetydelig (Mindre forstyrrelser i d) ▼ 2             |
| <b>INFORMASJONSSIKKERHET OG PERSONVERN</b><br>Moderat - Hendelsen kan føre til persc ▼ 6 | <b>INFORMASJONSSIKKERHET OG PERSONVERN</b><br>Moderat - Hendelsen kan føre til persc ▼ 6 |
| <b>OMDØMME</b><br>2 - Begrenset (naboer/brukere snakke) ▼ 4                              | <b>OMDØMME</b><br>2 - Begrenset (naboer/brukere snakke) ▼ 4                              |

☒ Akseptert

Lagre Slett

Kilde: skjermtutklipp fra kvalitetssystemet tatt 14.8.2026.

Fagansvarlig digitalisering forteller i intervju at når risikoanalyser gjennomføres, så deltar ansatte som har kjennskap til og har ansvar for løsningen som risikovurderes. I kun én av de seks risikovurderingene revisjonen har mottatt står det hvem som har deltatt i vurderingen ut over hvem som er ansvarlig for risikovurderingen og hvem som har stått for vurderingen av analysen. I dokumentasjonen revisjonen har mottatt kommer det dermed ikke fram om risikovurderingen er gjort kun av én person eller om det var flere som deltok i vurderingen.

Fagansvarlig IKT-sikkerhet og fagansvarlig digitalisering forteller begge i intervju at kommunen gjennomfører organisatoriske risikovurderinger, mens DGI gjennomfører tekniske risikovurderinger. Sikkerhetssjefen i DGI forteller i intervju at de tekniske risikovurderingene som DGI gjennomfører ikke uten videre er tilgjengelige for kommunene, da de kan inneholde sensitiv informasjon. Eksempelvis kan det avdekkes svakheter som uvedkommende ikke må vite om før risikoreduserende tiltak er gjennomført. Revisjonen har ikke etterspurt dokumentasjon på tekniske risikovurderinger gjennomført av DGI.

Kommunalsjef helse og mestring forteller i intervju at Nannestad kommune også deltar i risikovurderinger i samarbeid med de andre kommuner, både i DGI-samarbeidet og i andre interkommunale samarbeid. For eksempel er kommunene i samarbeidet i prosess med å anskaffe ny elektronisk pasientjournal. Dette er en stor anskaffelse i samarbeid mellom 18 kommuner. Arbeidet med anskaffelsen ledes av Lillestrøm kommune.

Personvernombud forteller i intervju at hun mener Nannestad kommune er gode på risikovurderinger, særlig knyttet til anskaffelser. Både det faste personvernombudet og vikarierende personvernombud har deltatt i risikovurderinger i Nannestad kommune. Personvernombudene forteller at de både deltar i selve gjennomgangen av risikovurderingene og at de får gjennomførte risikovurderinger til gjennomlesning. Personvernombudet utarbeidet en årsrapport om personvernarbeidet i Nannestad for 2024<sup>3</sup>, etter å ha vært ombud i Nannestad i ett år. I årsrapporten skriver hun at det er gjennomført et godt arbeid med risikoanalyser og vurderinger av personvernkonsekvenser i Nannestad kommune, i tillegg til at Nannestad har deltatt i flere risikovurderinger i DGI-samarbeidet.

## **2.3 Vurderinger av personvernkonsekvenser (DPIA)**

Ifølge artikkel 35 i personvernforordningen skal kommunen gjennomføre vurderinger av personvernkonsekvenser (DPIA) dersom en behandling av personopplysninger vil medføre høy risiko for personers rettigheter og friheter. Denne vurderingen skal som et minimum inneholde en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålet med behandlingen, en vurdering av om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålet, en vurdering av risiko for de registrertes rettigheter og friheter, og om de planlagte tiltakene for å håndtere risikoene og for å påvise at personvernreglene overholdes.

---

<sup>3</sup> Personvernombudet hadde etter dette vikar ett års tid og det ble da ikke utarbeidet årsrapport for 2025. Personvernombudet er nå tilbake i stillingen og forteller i intervju med revisjonen at hun vil fortsette med årsrapporter fremover.

Vurderinger av personvernkonsekvenser (DPIA) inngår i samme prosedyre som prosedyren for risikovurderinger omtalt over (DGI-kommunene 2025). I tillegg har kommunen en excel-mal for DPIA, da DPIA ikke gjennomføres i kvalitetssystemet. Malen inneholder en initialvurdering som brukes til å vurdere om det er nødvendig å gjennomføre en full DPIA. Dersom konklusjonen etter initialvurderingen er at det ikke er behov for å gjennomføre DPIA skal behandlingsansvarlig signere. Dersom initialvurderingen konkluderer med at det er behov for å gjennomføre DPIA skal det etter malen gjøres en systematisk beskrivelse av behandlingen av personopplysninger, en vurdering av nødvendighet og proporsjonalitet og en konsekvensutredning. Deretter skal de registrertes synspunkter hentes inn og personvernombudet skal gi en vurdering. Deltakerne skal registrere sin konklusjon på DPIA, og deretter skal leder vurdere og konkludere før behandlingsansvarlig skal signere. Malen inneholder også en møte- og endringslogg.

Kommunen har også en sjekkliste for DPIA som er utarbeidet i DGI-samarbeidet. Sjekklisten er utarbeidet for å sikre at kravene til DPIA er møtt, ved at alle temaene som er påkrevd etter personvernforordningen blir belyst ved å fylle inn sjekklisten. I sjekklisten står det at både gjennomført DPIA og sjekklisten skal forelegges personvernombudet for uttalelse og at begge dokumentene skal lagres i kommunens arkivsystem (DGI-kommunene 2019). Kommunen opplyser om at sjekklisten ikke er brukt i de fire DPIAene som revisjonen har mottatt, kun mal for DPIA. Kommunen opplyser videre om at DPIA-malen som brukes i dag har flere og bedre ledetekster enn tidligere malen (e-post til revisjonen 23.9.2026).

Fagansvarlig IKT-sikkerhet forteller i intervju at hun alltid er med når det gjennomføres DPIA. For å sikre kompetanse på personvern blir også personvernombudet koblet på i gjennomføringen av DPIA. Personvernombudet forteller i intervju at malen Nannestad kommune bruker for gjennomføring av DPIA er god og at hun har deltatt på flere gjennomføringer av DPIA i kommunen.

Revisjonen etterspurte eksempler på DPIA som er gjennomført i kommunen og på ulike tjenesteområder og har mottatt fire DPIA. Fagansvarlig IKT-sikkerhet forteller i intervju at det stort sett er på helseområdet det gjennomføres DPIA, men revisjonen har også mottatt DPIA knyttet til skole, tildeling av kommunale boliger og tilrettelagte tjenester. I en av disse ble det etter en initialvurdering konkludert med at det ikke er nødvendig å gjennomføre en full DPIA. For de tre andre vurderingene ble en full DPIA gjennomført. En av vurderingene er fullført med innhenting av de registrertes synspunkter, personvernombudets kommentar og signatur, samt aksept av restrisiko. De to øvrige vurderingene fremstår som uferdige, da de ikke inneholder uttalelser og aksept av restrisiko. Endringsloggen med informasjon om når DPIA er gjennomført og hvem som deltok i vurderingen er ikke fylt ut i de fire DPIA revisjonen har gjennomgått.

## **2.4 Revisjonens vurdering**

Revisjonens vurdering er at Nannestad kommune har etablert rutiner og praksis for gjennomføring av risikovurderinger om personvern og informasjonssikkerhet. Revisjonen mener imidlertid at det er noen forbedringspunkter.

Risikovurderinger gjennomføres i kommunens kvalitetssystem og kommunen har en fagansvarlig for IKT-sikkerhet som deltar i alle risikovurderinger og vurderinger av personvernkonsekvenser. I risikovurderingene revisjonen har mottatt blir risikoreduserende tiltak identifisert, og det blir delegert

ansvar for å gjennomføre tiltakene og det blir satt frister for gjennomføring. Når alle tiltak er gjennomført er det nærmeste leder som aksepterer restrisiko. I to av risikovurderingene er det flere av tiltakene som ikke er fullførte selv om fristen for gjennomføring er utløpt og restrisiko er markert som akseptert. Et annet forbedringspunkt er at risikovurderingene ofte ikke inneholder informasjon om tidspunkt for gjennomføring og hvem som har deltatt i risikovurderingen ut over den den som er ansvarlig for risikovurderingen og hvem som har stått for vurderingen av analysen. Mangelfull loggføring av dato og deltakere kan gjøre det utfordrende å følge opp ROS-arbeidet, særlig ved endringer i bemanning.

Revisjonens vurdering er at kommunen både har skriftlige rutiner for, og praksis for å gjennomføre, vurderinger av personvernkonsekvenser (DPIA). Noen av DPIAene revisjonen har gjennomgått er imidlertid mangelfullt dokumentert, særlig når det gjelder uttalelser, deltakere i gjennomgangen og hvorvidt restrisiko er akseptert.

## 3 SIKRING AV PERSONOPPLYSNINGER

### 3.1 Problemstilling og revisjonskriterier

Enhver har rett til å bestemme over egne personopplysninger. Kommunen er ansvarlig for å sikre personopplysningene til både innbyggere som bruker kommunens tjenester og for egne ansatte. Dersom kommunen ikke sørger for at personopplysninger som er registrert i kommunens systemer er sikret i tilstrekkelig grad, kan opplysningene komme på avveie. Dette kan både ha konsekvenser for den enkelte og konsekvenser for kommunen i form av tap av tillit og gebyrer fra Datatilsynet (NOU 2022:11, 59).

Kommunene må blant annet sørge for å ha kontroll på ansvarsforholdene mellom kommune og leverandører, ha oversikt over hvilke personopplysninger som behandles og sørge for at personopplysningene til elevene ikke kommer på avveie (Datatilsynet 2025).

For problemstilling 2 utledes følgende krav og forventninger til kommunen:

| Problemstilling 2                                                                                                | Krav og forventninger til kommunen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Har kommunen sørget for at personopplysninger som lagres i kommunens IT-systemer er sikret i tilstrekkelig grad? | <p>Kommunen skal ha</p> <ul style="list-style-type: none"> <li>→ internkontroll med personvern og informasjonssikkerhet, herunder <ul style="list-style-type: none"> <li>○ styrende dokumenter for informasjonssikkerhet og personvern</li> <li>○ tydelig rolle- og ansvarsfordeling knyttet til personvern</li> <li>○ gjennomføre ledelsens gjennomgang</li> </ul> </li> <li>→ protokoll over hvilke personopplysninger kommunen behandler (behandlingsprotokoll)</li> <li>→ dokumenterte rutiner som bidrar til å sikre kontroll på identiteter og tilganger</li> <li>→ etablert sikkerhetsovervåkning, og det bør gjennomføres analyser av data fra overvåkingen</li> <li>→ gjennomført inntrengingstester jevnlig</li> <li>→ rutiner og praksis som bidrar til å sørge for at kommunen har databehandleravtaler med eksterne leverandører som behandler personopplysninger</li> <li>→ tiltak som sikrer at ansatte får opplæring i personvern</li> </ul> |

## 3.2 Internkontroll med informasjonssikkerhet og personvern

### 3.2.1 Grunnleggende krav på området

Kommunen skal ha internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Videre bør internkontrollen være en integrert del av virksomhetens helhetlige styringssystem. (eForvaltningsforskriften § 15). Det finnes flere ulike standarder og rammeverk for styringssystem for informasjonssikkerhet. Digitaliseringsdirektoratet anbefaler at offentlige virksomheter i Norge baserer seg på standarden Ledelsessystemer for informasjonssikkerhet – krav (NS-ISO/IEC 27001). Standarden stiller en rekke krav til gjennomføring av aktiviteter for å sikre tilfredsstillende styring av informasjonssikkerhet, blant annet hvorvidt kommunen har på plass styrende dokumenter for informasjonssikkerhet og om kommunen har en klar oppgave-, rolle- og ansvarsfordeling på området. Som en del av internkontrollen er det også anbefalt å gjennomføre ledelsens gjennomgang av informasjonssikkerhet i kommunens øverste ledelse, for å bidra til at ledelsen får en jevnlig oppdatering på status for arbeidet med informasjonssikkerhet og personvern i organisasjonen og forankring i ledelsen (Digdir 2025, KS 2025).

### 3.2.2 Styringsdokumenter

Nannestad kommune har flere styringsdokumenter knyttet til informasjonssikkerhet og personvern som er utarbeidet i DGI-samarbeidet. Styringsdokumentene er lagret i kommunens kvalitetssystem.

Som et overordnet styringsdokument har DGI-kommunene en strategi for IKT-sikkerhet og personvern. Revisjonen har mottatt strategien som sist ble godkjent i 2021, samt en revidert strategi utarbeidet i 2026. Strategien fra 2021 inneholder blant annet beskrivelser av roller og ansvar. Rollene som beskrives er behandlingsansvarlig, personvernombudet, IKT-sikkerhetsansvarlig og IKT-sikkerhetsutvalget (i ny styringsmodell kalt IKT-sikkerhetsforum). Strategien inneholder også en beskrivelse av hva som skal gjennomgås i ledelsens gjennomgang. Kommunalsjefene, som inngår i kommunedirektørens ledergruppe, informerer imidlertid om at det ikke gjennomføres ledelsens gjennomgang av informasjonssikkerhet og personvern i Nannestad kommune. Den nye sikkerhetsstrategien som er utarbeidet i DGI-samarbeidet i 2026 inneholder mål og strategiske fokusområder for samarbeidet. Den nye strategien inneholder ikke de andre elementene fra 2021-strategien, som beskrivelser av roller og ansvar og ledelsens gjennomgang. Kommunen opplyser om at den reviderte strategien fra 2026 erstatter strategien fra 2021 (e-post til revisjonen 23.9.2026).

Ifølge strategien for IKT-sikkerhet og personvern, samt personvernerklæringen på kommunens hjemmeside slik den står per august 2026, er kommunedirektøren behandlingsansvarlig i kommunen. Kommunen presiserer imidlertid i e-post til revisjonen 4.9.2026 at det er kommunen som juridisk person som er behandlingsansvarlig.

DGI-kommunenes strategiske fokusområder er ifølge strategien å sikre god kompetanse på informasjonssikkerhet og personvern, å sikre at arbeidet med informasjonssikkerhet og personvern blir dokumentert og å sørge for en risikobasert tilnærming. Strategien viser til at det er kommunedirektørene i samarbeidet som er ansvarlige for det strategiske arbeidet og sikre at relevant kompetanse involveres (DGI-kommunene 2026).

Kommunen har en instruks for informasjonssikkerhet og personvern som er utarbeidet gjennom DGI-samarbeidet. Instruksen skal signeres av alle ansatte ved ansettelse i kommunen. Hensikten med instruksen er at alle ansatte i kommunene skal forstå sitt ansvar ved bruk av kommunens IT-utstyr og -løsninger for å forebygge at informasjon kommer på avveie, blir manipulert eller utilgjengelig. Ifølge instruksen har alle ansatte plikt til å forhindre at uvedkommende får tilgang til personopplysninger eller annen sensitiv informasjon. Instruksen stiller krav til ansattes bruk av digital kommunikasjon, håndtering av påloggingsinformasjon, fysisk sikring og gjennomgår prosedyrer for avslutning av arbeidsforhold. Ifølge instruksen skal ansatte som blir oppmerksomme på et mulig sikkerhetsbrudd varsle nærmeste leder, samt DGI eller den som er kommunens IKT-sikkerhetsansvarlig. Instruksen stiller krav til hvordan ansatte bruker kommunens IT-utstyr og kommunens nett. Ifølge instruksen skal DGI føre en liste over programmer og applikasjoner som ikke skal brukes av ansatte. Denne listen bli tilgjengeliggjort når den er klar. Etter hva revisjonen har kjennskap til har ikke DGI en slik liste i dag (DGI-kommunene 2023).

Revisjonen har videre mottatt flere prosedyrer utarbeidet i DGI-samarbeidet som er en del av kommunens internkontroll med informasjonssikkerhet og personvern. Prosedyrene er lagret i kommunens kvalitetssystem. Prosedyrene revisjonen har mottatt er:

- Prosedyre for bruk av kommunens digitale samhandlingsplattform
- Prosedyre for bruk av IKT-utstyr ved reise
- Prosedyre for risikovurderinger og vurderinger av personvernkonsekvenser
- Prosedyre for systemtilgang til ansatte – inn- og utmelding
- Prosedyre for å starte behandling av personopplysninger
- Prosedyre for bruk av LawAI (et verktøy basert på kunstig intelligens som brukes i HR)

I tillegg har kommunen et delegeringsreglement (2024), et styringsdokument knyttet til internkontroll for helse, miljø- og sikkerhet i kommunen, samt en digital utviklingsstrategi. Revisjonen kan imidlertid ikke se at informasjonssikkerhet og personvern er nevnt spesifikt i disse dokumentene.

### **3.2.3 Roller og ansvar**

Roller og ansvar for informasjonssikkerhet og personvern internt i kommunen følger i styringsdokumentene den generelle delegeringen via linjeledelsen (jf. kommunens delegeringsreglement). Kommunedirektøren har det overordnede ansvaret, og henholdsvis kommunalsjefer, virksomhetsledere og enhetsledere har det delegerte ansvaret for å følge opp sine tjeneste- og fagområder. Revisjonen blir opplyst i intervjuer om at delegeringsreglementet i Nannestad ikke er oppdatert, men at det pågår et arbeid med å oppdatere reglementet.

Kommunedirektøren har det overordnede ansvaret for internkontrollen i kommunen, og da også for informasjonssikkerhet og personvern. Kommunedirektørens rolle som kommunens behandlingsansvarlig er beskrevet i kommunens strategi for IKT-sikkerhet og personvern. Kommunedirektørene er også det øverste leddet i styringsmodellen i DGI-samarbeidet (porteføljestyret).

I intervjuer med kommunalsjefene i kommunen fortelles det at informasjonssikkerhet ikke er en fast sak på agendaen i kommunedirektørens ledergruppe, men at saker knyttet til temaet kommer opp ad hoc og etter behov. Revisjonen får opplyst i intervju med fagansvarlige og kommunalsjefer at det

ikke gjennomføres ledelsens gjennomgang av informasjonssikkerhet og personvern i kommunedirektørens ledergruppe. Sikkerhetssjefen i DGI forteller at han har ledelsens gjennomgang av informasjonssikkerhet for styret i DGI, men at denne gjennomgangen handler om hvordan DGI som selskap jobber med informasjonssikkerhet, og inkluderer ikke sikkerhetsarbeidet som skjer i hver enkelt kommune.

I intervjuer med kommunalsjefer pekes det på at informasjonssikkerhet og personvern er viktige lederansvar innenfor de ulike tjenesteområdene og det vises til at tjenesteområdene følger prosedyrene som DGI-kommunene har utarbeidet sentralt. Kommunalsjefene har det overordnede ansvaret for sine tjenesteområder, mens virksomhetslederne og enhetslederne har ansvar for sine enheter. De ulike tjenesteområdene har en digitaliseringsrådgiver som har 20 prosent av sine stillinger knyttet til kommunens digitaliseringsteam som representerer for sine respektive tjenesteområder. Fagleder digitalisering, som leder digitaliseringsteamet, forteller i intervju at hennes rolle som fagleder digitalisering ikke har spesielle oppgaver tilknyttet informasjonssikkerhet, men at informasjonssikkerhet er en del av digitaliseringsarbeidet. Fagansvarlig digitalisering forteller i intervju at hun rapporterer kommunedirektørens ledergruppe en gang i måneden. Alle digitale initiativer digitaliseringsteamet jobber med blir ifølge fagansvarlig digitalisering sendt til ledergruppen for godkjenning før de tas med inn i DGI-samarbeidet.

En ressurs direkte knyttet til informasjonssikkerhet og personvern er rollen som fagansvarlig for IKT-sikkerhet. Denne rollen er beskrevet i kommunens strategi for IKT-sikkerhet fra 2021 og inngår i styringsmodellen i DGI-samarbeidet. Fagansvarlig IKT-sikkerhet sitter i IKT-Sikkerhetsforum i DGI-samarbeidet.

Både fagansvarlige for digitalisering og IKT-sikkerhet og kommunalsjefer forteller i intervju at de opplever rolle- og ansvarsforholdet mellom kommunen og DGI som uklart. I intervjuene vises det til at rolle- og ansvarsfordelingen mellom kommunen og DGI har blitt noe klarere etter at ny styringsmodell for DGI-samarbeidet ble vedtatt, men at det fortsatt oppleves som uklart hvem som har ansvar for hva på flere områder. Blant annet trekkes det fram at det oppleves som uklart hva det er kommunene selv har ansvar for når det gjelder hva kommunen må eie og sikre selv og hva som kan overlates til DGI.

I flere av intervjuene kommer det fram at det er uklart hvem i kommunen som har ansvar for å holde seg informert om arbeidet med informasjonssikkerhet og personvern som skjer i DGI. IKT-sikkerhetsansvarlig er informert om arbeidet som skjer i IKT-Sikkerhetsforum og kommunedirektøren blir informert om det som blir presentert for porteføljestyret i DGI-samarbeidet. På spørsmål om hvem som holder seg oppdatert på tema som hvilke avtaler DGI har med sine underleverandører (se kap. 3.7), hendelser knyttet til kommunens sikkerhetsovervåkning (se kap. 3.5.) eller sikkerhetsarbeidet som gjøres i DGI som selskap er ikke dette klart for de fagansvarlige og kommunalsjefene revisjonen har intervjuet.

Kommunen har et personvernombud som har en rådgivende rolle i alle spørsmål knyttet til personvern. Personvernombudets rolle er beskrevet i kommunens strategi for IKT-sikkerhet og personvern fra 2021. Revisjonen har intervjuet både det faste personvernombudet og personvernombudet som vikarierte fra april 2025 til februar 2026. De forteller i intervju at de kontaktes av kommunen ved behov og at de er avhengige av at kommunene kontakter dem når det

er behov for bistand. Det faste personvernombudet leverte en årsrapport om sitt arbeid til kommunedirektøren i Nannestad i 2024. Det ble ikke laget årsrapport for 2025 da det var et vikarierende personombud mesteparten av året, men hun forteller at hun vil videreføre praksisen med årsrapportering fremover.

Nannestad kommune har ikke en personvernrådgiver. Ansvar for rådgivning om personvern er lagt til fagansvarlig IKT-sikkerhet (e-post til revisjonen 23.9.2026). Dette innebærer at fagansvarlig IKT-sikkerhet får spørsmål fra ulike tjenesteområder i kommunen i personvernspørsmål, og at personvernombudene blir kontaktet i spørsmål som tidligere ville gått til personvernrådgiveren.

Det faste og det vikarierende personvernombudet forteller begge i intervju at tiden deres «spises opp» av mindre oppgaver kommunen ber dem om bistand til. Personvernombudene forteller at de ønsker at kommunene de jobber for har egne personvernrådgivere, slik at personvernombudenes tid kan frigjøres til de mer overordnede oppgavene og jobbe på et mer risikobasert nivå.

### **3.3 Protokoll over personopplysninger (behandlingsprotokoll)**

Etter personvernforordningen artikkel 30 skal den behandlingsansvarlige føre protokoll over behandlingsaktiviteter som utføres under deres ansvar. Å føre protokoll over alle behandlinger av personopplysninger som gjøres i kommunen er viktig for å få oversikt over alle fagsystemer og prosesser hvor innbyggere og ansattes personopplysninger blir behandlet. En oppdatert oversikt er for eksempel viktig dersom det skjer et datainnbrudd og kommunen raskt må finne ut av hvilke personopplysninger de ulike fagsystemene behandler, eller dersom innbyggere ønsker innsyn i hvilke personopplysninger kommunen har om vedkommende.

Fagansvarlig IKT-sikkerhet forteller i intervju at kommunen før hadde et system for føring av protokoll over behandlinger av personopplysninger, men at lisensen til denne programvaren gikk ut uten å bli fornyet. Fagansvarlig forteller at hun tok ut en kopi av protokollen i en excel-fil før lisensen gikk ut. Revisjonen har mottatt denne filen.

I kommunens behandlingsprotokoll er det 296 registreringer. De fleste er opprettet i perioden 2021-22. Tre registreringer er opprettet i 2024. Sett bort fra de tre registreringene som ble lagt inn i 2024 er det ingen registreringer som er oppdatert siden 2022.

DGI-kommunene har en felles prosedyre for å starte behandling av personopplysninger som revisjonen har mottatt. Prosedyren forklarer hva personopplysninger er, definerer hva som regnes som særlige kategorier av personopplysninger som er særlig beskyttelsesverdig og forklarer hva som menes med behandling av personopplysninger. Videre gjennomgår prosedyren hvilke vurderinger, avklaringer og dokumentasjon som skal gjøres ved behandling av personopplysninger. Siste punkt i prosedyren er å oppdatere behandlingsprotokollen. I prosedyren står det at behandlingsprotokollen skal revideres løpende ved endringer, herunder ved organisasjonsendringer eller ved anskaffelse av nye systemer, og minst én gang i året. Ansvarlig for alle punktene i prosedyren er kommunalsjef, enhetsleder eller virksomhetsleder (DGI-kommunene 2022a).

Ingen av personene revisjonen har intervjuet i forbindelse med denne undersøkelsen har vært involvert i arbeidet med behandlingsprotokollen og det er usikkerhet knyttet til hvem som er ansvarlig for protokollen i dag. Kommunalsjefene som er intervjuet, har lite kjennskap til

behandlingsprotokollen og flere opplever at det ikke er tydelig kommunisert at det er et lederansvar å følge opp protokollen. En av de som ble intervjuet forteller at det var mer struktur i arbeidet med behandlingsprotokollen da kommunen hadde en personvernrådgiver, men at det nå er uklart hvem som skal følge opp protokollen.

Personvernombudet trakk fram arbeidet med behandlingsprotokollen i sin årsrapport for 2024. Her skriver hun at det forrige personvernombudet har arbeidet med protokollen, men at protokollen er lite kjent og at hun anbefaler at alle ledere har et bevisst forhold til protokollen og kan bruke denne aktivt i arbeidet med personvern (Personvernombudet i Nannestad 2024).

### **3.4 Kontroll på identiteter og tilganger**

Ett av NSMs grunnprinsipper for IKT-sikkerhet er prinsippet om å ha kontroll på identiteter og tilganger. Dette er viktig fordi manglende kontroll på tilganger øker risikoen for dataangrep. Prinsippet innebærer blant annet å etablere retningslinjer for tilgangskontroll (NSM 2024).

Kommunen har en prosedyre for systemtilgang til ansatte som har til hensikt å sikre at sikkerhet og personvern ivaretas i kommunen ved å sørge for at ansatte gis tilgang til nettverk, systemer og filområder ut fra til enhver tid tjenstlig behov, samt at tilganger deaktiveres når tjenstlig behov opphører. Behov for tilganger meldes til nærmeste leder. Prosedyren presiserer at det ikke skal gis flere tilganger enn det som er den ansattes tjenstlige behov. Tilganger bestilles via DGIs bestillingssystem. Ansvarlig for å deaktivere den ansattes tilganger når arbeidsforholdet opphører er lagt til leder med personalansvar (DGI-kommunene 2022b).

Fagansvarlig digitalisering forteller i intervju at tilgangsstyringen er automatisert og styres av DGI. I tillegg har kommunen systemansvarlige for hvert enkelt system, som kan gi tilgang til de som har behov. Videre kan ledere i kommunen bestille tilganger. Når leder bestiller en tilgang, går det ifølge fagansvarlig et varsel til en systemansvarlig i kommunen. Systemansvarlig må da manuelt opprette brukeren i systemet.

Kommunalsjef for helse og mestring forteller i intervju at de har strenge regler for tilgangsstyring av den elektroniske pasientjournalen, og at tilgang gis basert på behovet den aktuelle ansatte har for tilgang til pasientinformasjon. Enhetslederne har ansvar for å slette brukere som slutter i stillingene sine. Der er imidlertid ikke alltid dette blir gjort, og de har derfor jevnlig gjennomgang av brukere av den elektroniske pasientjournalen. Gjennomgangen gjennomføres av en konsulent som er systemansvarlig for den elektroniske pasientjournalen i kommunen.

Kommunalsjef for oppvekst forteller i intervju at de har en ressurs som har et særlig ansvar knyttet til IKT-sikkerhet, og som blant annet har ansvar for tilgangsstyringen av Feide<sup>4</sup>. En konsulent ved ungdomsskolen har rolle som superbruker for skolens administrasjonssystem.

Fagansvarlig IKT-sikkerhet forteller i intervju at de fleste systemer som brukes i kommunen driftes av DGI, men at det finnes noen systemer med kun en eller to brukere i kommunen som ikke er driftet av DGI. I flere av intervjuene som er gjennomført i denne undersøkelsen vises det til at det er satt i

---

<sup>4</sup> Nasjonal fellesløsning for sikker innlogging. Feide er en tjeneste for enhetlig identitetsforvaltning i norsk utdanningssektor.

gang en kartlegging av såkalt «skygge-IT». Fagansvarlig digitalisering forteller at skygge-IT i denne sammenhengen er de anskaffelsene som er gjort innad kommunen og som håndteres innad i kommunen uten involvering av DGI. Det er digitaliseringsteamet som gjennomfører denne kartleggingen. Sikkerhetssjefen i DGI forteller at det er DGI som har initiert kartleggingen av såkalt skygge-IT da DGI ser på det som en sikkerhetsutfordring at kommunene ikke har oversikt over alle systemene og underleverandørene som brukes i kommunenes tjenesteområder.

### **3.5 Sikkerhetsovervåkning**

Sikkerhetsovervåkingen av kommunens IT-systemer blir gjennomført av et sikkerhetsoperasjonssenter (SOC) som leveres av DGIs driftsleverandør. Revisjonen har mottatt driftsavtalen mellom DGI og leverandøren av driftstjenester. Avtalen ble signert i 2018.

IKT-sikkerhetsansvarlig forteller i intervju at det er lite informasjonsoverføring mellom kommunene i DGI-samarbeidet og leverandøren som står for sikkerhetsovervåkingen. IKT-sikkerhetsansvarlig kjenner ikke til om kommunen får rapporter om overvåkingen. Det kommer også frem i intervjuene med kommunalsjefene at det er lite kjennskap til hvem i kommunen som eventuelt mottar rapporter om sikkerhetsovervåkingen eller hvordan kommunen blir varslet ved hendelser knyttet til IKT-sikkerhet.

I intervju med sikkerhetssjefen i DGI går det frem at det ikke er noe systematikk på informasjonsutvekslingen mellom kommunene og DGI når det gjelder funn fra sikkerhetstester, rapporter fra overvåking og hendelser fra SOC osv. DGI får rapporter om hendelser fra underleverandøren, men kommunene får ikke oversendt disse rapportene.

### **3.6 Inntrengingstester**

Ett av NSMs grunnprinsipper for IKT-sikkerhet er at det gjennomføres inntrengingstester jevnlig, og minst en gang i året, for å identifisere sårbarheter (NSM 2024).

Sikkerhetssjefen i DGI forteller i intervju at det er gjennomført inntrengingstester i 2022, 2023 og 2024, men det er ikke gjennomført etter dette. Han peker imidlertid på at denne typen sikkerhetstiltak er kostbare, og økonomi legger noe begrensning på hvor ofte og i hvor stort omfang inntrengingstester gjennomføres. Han mener imidlertid at testene er viktige, da testene avdekker en del svakheter i IT-systemene. Sikkerhetssjefen forteller at det jevnlig blir gjennomført sikkerhetstiltak på systemene som administreres av DGI, blant annet sårbarhetstester på samhandlingsplattformen.

### **3.7 Databehandleravtaler**

Ifølge personvernforordningen skal behandlinger av personopplysninger utført av en databehandler være underlagt en bindende avtale mellom databehandleren og den behandlingsansvarlige. Kommunen er behandlingsansvarlig, men databehandleravtaler signeres også mellom DGI og DGIs underleverandører. Avtalen skal fastsette gjenstanden for og varigheten av behandlingen, behandlingens art og formål, typen personopplysninger og kategorier av registrerte, samt den behandlingsansvarliges rettigheter og plikter (se vedlegg 2 for en detaljert beskrivelse av kravene til innhold i databehandleravtaler jf. personvernforordningens artikkel 28).

Ifølge kommunens strategi for IKT-sikkerhet og personvern skal ekstern behandling av personopplysninger være regulert i en databehandleravtaler før behandlingen kan begynne (DGI-kommunene 2021). Revisjonen har mottatt malen for databehandleravtaler som benyttes av DGI-kommunene, herunder Nannestad kommune. Malens innhold ivaretar etter revisjonens oppfatning kravene i personvernforordningens artikkel 28.

I intervjuene revisjonen har gjennomført opplyses det om at malen for databehandleravtaler i hovedsak blir brukt, men at leverandørens egen mal i noen tilfeller blir brukt dersom denne malen tilfredsstiller kriteriene i DGI-kommunenes egen mal.

Revisjonen har mottatt et eksempel på en signert databehandleravtale mellom kommunen og leverandør av en digital tjeneste. Avtalen er ikke ført etter kommunens mal, men innholdet dekker kravene til databehandleravtaler i personvernforordningen og i kommunens egen mal.

Kommunalsjefene forteller i intervju at de får tilsendt databehandleravtaler som de skal signere på, og at disse lagres i kommunens arkivsystem. En av kommunalsjefene forteller i intervju hun opplever det som vanskelig å forstå innholdet i databehandleravtaler hun blir bedt om å signere. Hun forteller at hun da ber om mer informasjon eller støtte til å forstå innholdet i avtalen, men at innholdet i avtalen fortsatt kan være uklart for henne selv etter flere runder.

Revisjonen har i tillegg til nevnte databehandleravtale over mottatt Nannestad kommunes databehandleravtale med DGI. Databehandleravtalen ble signert i 2013 i forbindelse med inngåelse av driftsavtalen. Databehandleravtalen mellom DGI og Nannestad kommune inneholder en liste over underleverandører. Siden signeringen av databehandleravtalen mellom DGI og kommunene har DGI satt ut driften av IT-systemene til en underleverandør, uten at avtalen mellom kommunene og DGI er endret. Både sikkerhetssjefen i DGI og personvernombudet trekker i intervju frem som en svakhet at avtalen med DGI, inkludert oversikten over DGIs underleverandører, ikke har blitt oppdatert eller revidert på flere år. Sikkerhetssjefen i DGI peker på at databehandleravtalen mellom DGI og kommunen ikke inneholder instruks om roller, ansvar og digital sikkerhet. Han viser også til at avtalen mellom kommunene og DGI bør synkroniseres med avtalene DGI gjør med sine underleverandører.

### **3.8 Opplæring i personvern**

Opplæring av ansatte er et sentralt tiltak for å sikre god informasjonssikkerhet i kommunen (KS 2022). Ifølge DGI-kommunenes instruks for informasjonssikkerhet og personvern skal ledere sørge for at ansatte har tilgang til og er kjent med tilgjengelig obligatorisk opplæring innen informasjonssikkerhet og personvern. Videre skal ansatte ifølge instruksen gjennomføre tilgjengelig obligatorisk opplæring innen informasjonssikkerhet og personvern (DGI-kommunene 2023). Revisjonen har imidlertid ikke mottatt dokumentasjon på at Nannestad kommune har obligatorisk opplæring innenfor temaene personvern og informasjonssikkerhet.

På kommunens ansattportal ligger en presentasjon fra kommunens nyansattdag i mai 2025. Presentasjonen inneholder en informasjon om IKT-sikkerhet og gir en innføring i hva informasjonssikkerhet og personopplysninger er, tiltak ansatte selv kan gjøre for å hindre at digitale verdier kommer på avveie, informasjon om personvernombudets rolle, samt informasjon om hva brudd på personopplysningssikkerheten kan være. Det ligger videre informasjon om

informasjonssikkerhet og personvern på kommunens ansattportal, inkludert opplæringsvideoer i personvern som er lagt ut på DGI-kommunenes fellessider. På ansattportalen lenkes det også til digitale informasjons- og opplæringsider som er tilgjengelig på nett.

Flere av de revisjonen har intervjuet savner et opplæringsopplegg knyttet til personvern og informasjonssikkerhet.

Fagansvarlig IKT-sikkerhet forteller i intervju at det tidligere har blitt kjøpt inn elektronisk opplæring. Denne opplæringen ble gjennomført av de ansatte i administrasjonen i Nannestad, men det var ifølge fagansvarlig få som gjennomførte opplæringen. Særlig innenfor helse, mestring og oppvekst var det liten svarprosent på den elektroniske opplæringen. En presentasjon av ledelsens gjennomgang av informasjonssikkerhet og personvern i DGI<sup>5</sup> bekrefter dette og viser at Nannestad kommune hadde en gjennomføringsgrad på 13 prosent, som er den laveste blant DGI-kommunene.

### 3.9 Revisjonens vurdering

Nannestad kommune har et styringssystem for informasjonssikkerhet og personvern, som i stor grad er basert på DGI-samarbeidet. Kommunens strategi for IKT-sikkerhet og personvern, samt prosedyrer knyttet til informasjonssikkerhet er utarbeidet i DGI-samarbeidet. Revisjonens inntrykk er imidlertid at roller og ansvar på flere områder er ikke tilstrekkelig avklart og at internkontrollen av informasjonssikkerhet og personvern ikke følges godt nok opp. Det er ikke gjennomført ledelsens gjennomgang av informasjonssikkerhet i kommunedirektørens ledergruppe.

Kommunen har en protokoll over behandlinger og personvern, men denne ikke er oppdatert og fulgt opp etter at den ble etablert. DGI-kommunenes prosedyre for behandlinger av personopplysninger, som også beskriver prosedyrene knyttet til behandlingsprotokollen, viser til at lederne er ansvarlige for å registrere behandlinger av personopplysninger i protokollen for sine fagområder, men dette synes ikke å være kjent for lederne selv. En konsekvens av å ikke ha en oppdatert oversikt over behandlinger av personopplysninger er at kommunen ikke er i stand til å raskt skaffe seg denne informasjonen ved et eventuelt dataangrep hvor det er mistanke om at personopplysninger kan ha kommet på avveie.

Revisjonens vurdering er at kommunen har dokumenterte rutiner som kan bidra til å sikre kontroll på identiteter og tilganger. Tilgangsstyringen skjer via DGI og tilgang til systemer gis ved at leder søker om tilgang for sine ansatte via DGIs bestillingssystem, samt at de ulike tjenesteområdene har dedikerte roller knyttet til å gi og følge opp ansattes tilganger til fagsystemene.

Revisjonens vurdering er at kommunen sørget for at det er på plass sikkerhetsovervåkning av systemene som driftes av eller via DGI. NSM anbefaler at kommunen analyserer data fra sikkerhetsovervåkingen. Kommunen mottar slik revisjonen oppfatter det ingen analyser eller rapporteringer fra sikkerhetsovervåkingen. Revisjonen mener at kommunens ansvar for informasjonssikkerhet og personvern ikke kan delegeres til en underleverandør. I henhold til god

---

<sup>5</sup> Sikkerhetssjefen i DGIs presentasjon for styret i DGI, ble også delt med kommunedirektørenes porteføljestyre (KDU-P) 28. april 2023.

internkontroll bør det som et minimum rapporteres til kommunen om sikkerhetshendelser og status for sikkerheten i kommunens IT-systemer.

Revisjonens vurdering er at det er gjennomført inntrengingstester, men at det ikke har vært gjennomført etter 2024. Revisjonen vil peke på at det er anbefalt å gjennomføre denne typen tester årlig.

Etter revisjonens vurdering har Nannestad kommune rutiner og praksis for som bidrar til å sikre at det inngås databehandleravtaler med eksterne som behandler personopplysninger på vegne av kommunen.

Revisjonens vurdering er at det mangler systematisk opplæring om personvern og informasjonssikkerhet i Nannestad kommune som sikrer at ansatte har kompetanse på og bevissthet rundt informasjonssikkerhet og personvern.

## 4 KONKLUSJON OG ANBEFALINGER

Undersøkelsen viser at Nannestad kommune har mye på plass når det gjelder arbeidet med informasjonssikkerhet og sikring av personopplysninger. Samtidig viser undersøkelsen at det er flere svakheter som bør utbedres. De viktigste manglene gjelder tydelige rolle-, ansvars- og oppgavebeskrivelser, at kommunen ikke har en oppdatert protokoll over behandling av personopplysninger og at kommunen ikke har tilstrekkelig systematisert opplæring i informasjonssikkerhet og personvern.

Kommunen gjennomfører risikovurderinger av informasjonssikkerhet og personvern, og disse følges langt på vei opp. Kommunen har imidlertid et forbedringspotensial knyttet til dokumentasjonen av DPIA som gjennomføres, særlig knyttet til innhenting av vurderinger, informasjon om deltakere og tidspunkt for gjennomgangene og aksept av restrisiko.

Revisjonens konklusjon er videre at kommunen i noen grad sikrer personopplysninger som er lagret i kommunens IT-systemer, men at det er mangler på flere områder. Etter revisjonens syn er ikke roller og ansvar knyttet til personopplysninger tilstrekkelig avklart. Dette gjelder blant annet arbeidet med kommunens behandlingsprotokoll, det overordnede ansvaret for å følge opp spørsmål knyttet til personvern og ansvaret for opplæring knyttet til personvern og informasjonssikkerhet.

Revisjonens inntrykk er at kommunen i stor grad lener seg på arbeidet som gjøres i DGI-samarbeidet og drift av IT-systemer gjennom DGI som selskap. Revisjonens oppfatning er at kommunen ikke i tilstrekkelig grad har tatt eierskap til sikring av personopplysninger internt i kommunen. Eksempelvis blir ledelsens gjennomgang av informasjonssikkerhet i DGI presentert for styret i DGI årlig, men det gjennomføres ikke ledelsens gjennomgang av informasjonssikkerhet i kommunens ledergruppe. En konsekvens av dette kan være at arbeidet med informasjonssikkerhet i DGI-samarbeidet blir synliggjort, men at det ikke er tilsvarende oversikt over informasjonssikkerheten internt i Nannestad kommune.

Kommunen har etter revisjonens syn ikke tilstrekkelig systematisert opplæring av ledere og ansatte i informasjonssikkerhet og personvern. Kommunen har enkelte opplæringstiltak, blant annet knyttet til nyansatte, men ut over dette er det revisjonens inntrykk at det er opp til den enkelte ansatte og den enkelte leder å holde seg oppdatert om informasjonssikkerhet og personvern.

Basert på det som kommer frem i undersøkelsen anbefaler revisjonen at kommunedirektør:

1. sørger for tilstrekkelig internkontroll med informasjonssikkerhet i Nannestad kommune, herunder
  - a. å gjennomføre ledelsens gjennomgang av informasjonssikkerhet årlig
  - b. å sikre en tydelig rolle- og ansvarsfordeling
2. sikrer at vurderinger av personvernkonsekvenser dokumenteres i tilstrekkelig grad
3. sikrer at kommunens protokoll over behandlinger av personopplysninger oppdateres og følges opp jevnlig
4. sørger for systematisk opplæring i personvern og informasjonssikkerhet

## LITTERATUR- OG KILDELISTE

### Lov, forskrift og veiledere

Lov om kommuner og fylkeskommuner av 22. juni 2018 nr. 83 (kommuneloven).

Lov om nasjonal sikkerhet av 1. juni 2018 nr. 24 (sikkerhetsloven).

Lov om behandling av personopplysninger av 15. juni 2018 nr. 38 (personopplysningsloven).

Forskrift om behandling av personopplysninger av 15. juni 2018 nr. 876.

Forskrift om elektronisk kommunikasjon med og i forvaltningen av 25. juni 2004 nr. 988 (eForvaltningsforskriften).

### Veiledere

Nasjonal sikkerhetsmyndighet (2024). NSMs grunnprinsipper for IKT-sikkerhet versjon 2.1, 2024.

Digitaliseringsdirektoratet (2025). Internkontroll i praksis – informasjonssikkerhet. Versjon 2.0. Hentet 13.8.2026 fra <https://www.digdir.no/informasjonssikkerhet/internkontroll-i-praksisinformasjonssikkerhet/2601>

KS (2025) Kommunedirektørens verktøykasse for informasjonssikkerhet. Et tillegg til Kommunedirektørens internkontroll – Orden i eget hus.

### Stortingsdokumenter

Meld. St. 38 2016-2027 IKT-sikkerhet - Et felles ansvar

NOU 2015:13 Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden.

### Dokumenter fra Nannestad kommune

Nannestad kommune (2024) Delegeringsreglement 2024-2027 fra kommunestyret, til formannskapet og utvalg m.fl. Vedtatt av Kommunestyret i PS 24/23, 19.03.2024. Revidering vedtatt av Kommunestyret i PS 24/71, 18.06.2024.

Nannestad kommune (udatert) Internkontroll helse, miljø og sikkerhet.

### Dokumenter utarbeidet i DGI-samarbeidet

DGI-kommunene (2019) Sjekkliste for personvernkonsekvensvurderinger (DPIA). Dokument-ID 10327-1.

DGI-kommunene (2021) Strategi for IKT sikkerhet og personvern for kommunene i Gardermoregionen. Sist revidert og godkjent av kommunedirektørene 17.02.2021.

DGI-kommunene (2022a) Prosedyre for å starte behandling av personopplysninger. Dokument-ID: 5918-4. Godkjent 17.6.2022 av kommunedirektørutvalget (KDU-P).

DGI-kommunene (2022b) Prosedyre for systemtilgang til ansatte - inn- og utmelding. Dokument-ID: 5902-5. Godkjent 27.6.2022 av kommunedirektørutvalget (KDU-P).

DGI-kommunene (2023) Instruks for informasjonssikkerhet og personvern. Dokument-ID 13332-6.

DGI-kommunene (2025) Digital utviklingsstrategi for kommunene i DGI-samarbeidet. Dokument-ID: 17114-1.

DGI-kommunene (2025) Prosedyre for risikovurderinger og vurderinger av personvernkonsekvenser. Dokument-ID: 17569-1.

DGI-kommunene (2026) Strategi for informasjonssikkerhet og personvern for kommunene i DGI-samarbeidet.

### **DGI (som selskap)**

DGI (2023) Ledelsens gjennomgang av informasjonssikkerhet og personvern i 2022. Delt med KDU-P 28. april 2023. Presentasjon.

### **Dokumenter fra personvernombudet**

Personvernombudet i Nannestad (2024) Årsrapport for personvernarbeidet i Nannestad kommune 2024.

### **Andre kilder**

Datatilsynet (2022) Overtredelsesgebyr til Østre Toten kommune. Hentet 10.8.2026 fra <https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2022/overtredelsesgebyr-til-ostre-toten-kommune/> [Hentet 10.8.2026]

Datatilsynet (2026a) Hva er en behandlingsansvarlig? Hentet 6.8.2026 fra <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsansvarlig-og-databehandler/hva-er-en-behandlingsansvarlig/>

Datatilsynet (2026b) Vurdering av personvernkonsekvenser (DPIA). Hentet 13.8.2026 fra <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdering-av-personvernkonsekvenser/>

Digdir (2026) Begrepsliste for informasjonssikkerhet. Hentet 13.8.2026 fra <https://www.digdir.no/informasjonssikkerhet/begrepsliste-informasjonssikkerhet/3230>

NAOB – Det norske akademis ordbok (2026) Informasjonssikkerhet. Hentet 13.8.2026 fra <https://naob.no/ordbok/informasjonssikkerhet>

NRK (2026) Her finner NRK stjålet info om mange tusen innbyggere. <https://www.nrk.no/stor-oslo/xl/folsom-info-om-tusenvis-av-innbyggere-ble-funnet-pa-det-morke-nettet-1.17963757> [Hentet 10.8.2026]

## VEDLEGG 1 REVISJONSKRITERIER

### Revisjonskriterier og kilder

Revisjonskriterier er de normer og krav som stilles til kommunens virksomhet som er omfattet av en forvaltningsrevisjon. Revisjonskriteriene er dermed målestokken som kommunens praksis vurderes opp mot. Revisjonskriterier kan utledes fra lover og forskrifter, kommunestyrets vedtak og hva som anses som god forvaltningsskikk og faglig anerkjente normer på området.

I denne undersøkelsen er revisjonskriteriene utledet fra følgende kilder:

- Lov om nasjonal sikkerhet av 1. juni 2018 nr. 24 (sikkerhetsloven)
- Lov om kommuner og fylkeskommuner av 22. juni 2018 nr. 83 (kommuneloven)
- Lov om behandling av personopplysninger av 15. juni 2018 nr. 38 (personopplysningsloven)
- Forskrift om behandling av personopplysninger av 15. juni 2018 nr. 876
- Forskrift om elektronisk kommunikasjon med og i forvaltningen av 25. juni 2004 nr. 988 (eForvaltningsforskriften)
- Veiledere basert på anerkjente standarder for informasjonssikkerhet:
  - Datatilsynets veileder «Virksomhetens plikter» ([nettbasert veileder](#))
  - Digitaliseringsdirektoratets (Digdir) veileder «Internkontroll i praksis – informasjonssikkerhet» ([nettbasert veileder](#))
  - Kommunal- og moderniseringsdepartementet (KMD) og Direktoratet for forvaltning og IKT (Digdir) 2015, Veileder til eForvaltningsforskriften, del 1. Elektronisk samhandling med og i forvaltningen – eForvaltningsforskriften. Rolf Riisnæs, advokat dr. juris, Wikborg, Rein & Co. Advokatfirma DA.
  - KS 2025. Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet. Et tillegg til Kommunedirektørens internkontroll – Orden i eget hus
  - NSMs grunnprinsipper for IKT-sikkerhet versjon 2.1, 2024
  - NSMs rammeverk for håndtering av IKT-sikkerhetshendelser

### Risikovurderinger

#### Generelt om internkontroll og risikovurderinger knyttet til informasjonssikkerhet og personvern

Kommunens styringssystem for informasjonssikkerhet skal ivareta kommunens internkontroll på området informasjonssikkerhet. Ifølge lov om kommuner og fylkeskommuner (kommuneloven) § 25-1 skal kommuner ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges. Etter paragrafens andre avsnitt skal internkontrollen være systematisk og tilpasses virksomhetens størrelse, egenart, aktiviteter og risikoforhold. Kommunedirektøren er ansvarlig for internkontrollen i kommunen og skal:

- a. utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering

- b. ha nødvendige rutiner og prosedyrer
- c. avdekke og følge opp avvik og risiko for avvik
- d. dokumentere internkontrollen i den formen og det omfanget som er nødvendig
- e. evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.

Sikkerhetsloven § 4-2 krever at virksomheten regelmessig skal gjennomføre vurdering av risiko. Vurderingen danner grunnlaget for iverksetting av forebyggende sikkerhetstiltak. Videre skal virksomheten kartlegge, som en del av vurderingen, hvilke virksomheter den er avhengig av for å fungere som den skal. Vurderingen skal gjennomgås jevnlig og om nødvendig revideres. Kravet om vurdering av risiko er videre utdypet i virksomhetsikkerhetsforskriften § 12. Forskriften skriver i andre ledd at behovet for å gjennomføre en ny helhetlig vurdering av risikoen skal vurderes årlig.

Etter forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) § 15 andre avsnitt skal kommunen som forvaltningsorgan ha en internkontroll på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør videre være en integrert del av virksomhetens helhetlige styringssystem. Tredje ledd § 15 krever at omfang og innretning på internkontroll skal være tilpasset risiko.

Digitaliseringsdirektoratet beskriver i sin veileder *Internkontroll i praksis – informasjonssikkerhet* vurderinger av risiko som «hjertet» i internkontrollen. Risiko som angår informasjonssikkerhet må ifølge veilederen identifiseres, analyseres og evalueres. Risikovurderingen kan gjelde hele kommunen på strategisk nivå, enkelte oppgaver eller tjenester, eller spesifikke informasjonssystemer eller deler av disse. Veilederen *Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet* (KS 2025) peker på viktigheten av å gjennomføre risikovurderinger for å få oversikt over mulige uønskede hendelser og bidra til at sikkerhets- og personvernarbeidet retter fokus mot områder med høyest risiko.

### **Risikoreducerende tiltak og restrisiko**

Etter at en risikovurdering er gjennomført skal risiko håndteres. Sikkerhetstiltak etableres og forvaltes for å redusere risiko, gjennom å redusere konsekvenser av uønskede hendelser eller sannsynligheten for at de inntreffer (Digdir-veilederen). Der hvor det er identifisert høy risiko må kommunedirektøren sikre at tiltak blir iverksatt, og forsikre seg om at risiko blir redusert (KS-veilederen).

Et av NSMs grunnprinsipper handler om å identifisere virksomhetens toleransegrenser for risiko knyttet til IKT. Dette innebærer at ledelsen må fastsette hvilke grenser for risiko kommunen aksepterer og hva som er uakseptabel risiko. I veilederen til KS vises det til at risikoforståelse og aksept av restrisiko er et lederansvar. Ifølge KS-veilederen bør kommunedirektøren som minimum kjenne til resultatet av risikovurderingene og ta stilling til uakseptabel risiko. Ifølge veilederen er det avgjørende at aksept av restrisiko besluttet og dokumenteres for å kunne jobbe risikobasert og prioritere tiltak for aktiviteter som innebærer høy risiko.

### **Vurdering av personvernkonsekvenser (DPIA)**

Personvernforordningens artikkel 35 krever at kommunen ved behandlinger som vil medføre høy risiko for fysiske personers rettigheter og friheter, skal gjennomføre en vurdering av

personvernkonsekvenser, også kalt DPIA (Data Protection Impact Assessment). Etter syvende punkt i artikkel 35 skal vurderingen skal minst inneholde:

- a. en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen
- b. en vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene
- c. en vurdering av risikoene for de registrertes rettigheter og friheter
- d. de planlagte tiltakene for å håndtere risikoene og for å påvise at personvernreglene overholdes

Det er krav om å utpeke et personvernombud, og kommunen skal rådføre seg med vedkommende i forbindelse med utførelsen av en vurdering av personvernkonsekvenser (artikkel 35, punkt 2).

Følgende revisjonskriterier legges til grunn for problemstilling 1:

| Problemstilling 1                                                                                                                       | Krav og forventninger til kommunen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gjennomføres det nødvendige risikovurderinger knyttet til informasjonssikkerhet og personvern og hvordan følges risikovurderingene opp? | <p>Kommunen skal ha</p> <ul style="list-style-type: none"> <li>→ rutiner og praksis som sikrer at det gjennomføres risikovurderinger knyttet til informasjonssikkerhet og personvern</li> <li>→ rutiner og praksis som sikrer at risikoreduserende tiltak etableres, gjennomføres og følges opp</li> <li>→ rutiner og praksis som sikrer at restrisiko aksepteres etter risikoanalyser og risikoreduserende tiltak</li> <li>→ rutiner og praksis som sikrer at det gjennomføres vurderinger av personvernkonsekvenser (DPIA)</li> </ul> |

## Personopplysninger

### Generelt om krav etter personopplysningsloven

Kommunens ansvar for forsvarlig håndtering av personopplysninger er regulert av personopplysningsloven. Personopplysningsloven gjennomfører EUs personvernforordning (GDPR) i norsk rett, jf. personopplysningsloven § 1. Formålet er å fastsette regler om vern av fysiske personer i forbindelse med behandling av personopplysninger, og regler om fri utveksling av personopplysninger. Personopplysningsloven og forordningen gjelder for helt eller delvis automatisert behandling av personopplysninger og for ikke-automatisert behandling av

personopplysninger dersom opplysningene inngår i eller skal inngå i et register, jf. personopplysningsloven § 2.

Kommunen behandler personopplysninger om både innbyggere og ansatte. For å ivareta en forsvarlig behandling av personopplysningene, plikter kommunen å sette i verk egnede tekniske og organisatoriske tiltak for å sikre og påvise at personopplysninger behandles i samsvar med regelverket, jf. personvernforordningen art. 24. Internkontrollen skal ivareta den registrertes rettigheter og friheter, og ivareta virksomhetens mål med behandlingen av personopplysningene. Tiltakene skal dokumenteres og oppdateres ved behov (ibid.).

Personopplysningene skal beskyttes mot uberettiget innsyn og endringer, men skal være tilgjengelige for de som trenger opplysningene, når de trenger dem (personvernforordningen artikkel 5).

Behandlingsansvarlig er en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes, jf. personvernforordningen art. 4. Det betyr at kommunen er behandlingsansvarlig for personopplysninger som kommunen samler inn og benytter. Det er kommunen som juridisk person som er behandlingsansvarlig. Ledelsen kan delegere oppgaver knyttet til behandling av personopplysninger, men selve behandlingsansvaret kan ikke delegeres (Datatilsynet 2026).

### **Internkontroll med personvern og informasjonssikkerhet**

Som ansvarlig for internkontrollen i kommunen skal kommunedirektøren utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering (kommuneloven § 25-1). Kommunedirektøren skal dokumentere internkontrollen i den formen og det omfanget som er nødvendig (§ 25-1 d). Kommunen skal ifølge kommuneloven § 25-1 ha nødvendige rutiner og prosedyrer og evaluere skriftlige prosedyrer og andre tiltak for internkontroll og forbedre disse ved behov. I KS-veilederen er kommunene anbefalt å utarbeide rutiner og prosedyrer for når, hvordan og hvem som skal utføre oppgaver. Kommunen anbefales å beskrive organiseringen av arbeidet, herunder roller og ansvar for sikkerhet og personvern.

Mens kommuneloven § 25-1 stiller krav til internkontroll i kommunen generelt, stiller eForvaltningsforskriften krav til internkontroll på informasjonssikkerhetsområdet spesielt. Kommunen skal etter forskriftens § 15 ha sikkerhetsmål og en sikkerhetsstrategi som beskriver mål og strategi for kommunens internkontroll.

Ifølge KS sin veileder *Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet* anbefales det at personvern og informasjonssikkerhet er en del av kommunens sektorovergripende internkontroll. En klar ansvarsfordeling, delegering og beskrivelse av roller er en vesentlig del av styringssystemet for personvern og informasjonssikkerhet. Ifølge KS-veilederen bør det fordeles og dokumenteres ansvar for informasjonsverdier, kritikalitet og behandlingsprotokoller, gjennomføring av risikovurderinger av ulike behandlinger og løsninger, personvernkonsekvensvurderinger og oppfølging av eksterne leverandører (KS 2025, s. 19).

## Behandlingsprotokoll

Artikkel 30 i personvernforordningen krever at kommunen fører protokoll over behandlingsaktiviteter. Behandlingsprotokollen skal ifølge artikkel 30 inneholde følgende informasjon:

- a. navnet på og kontaktopplysningene til den behandlingsansvarlige og, dersom det er relevant, den felles behandlingsansvarlige, den behandlingsansvarliges representant og personvernombudet,
- b. formålene med behandlingen,
- c. en beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger,
- d. kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, herunder mottakere i tredjestater eller internasjonale organisasjoner,
- e. dersom det er relevant, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon, herunder identifikasjon av nevnte tredjestat eller internasjonale organisasjon og, ved overføringer nevnt i artikkel 49 nr. 1 annet ledd, dokumentasjon på nødvendige garantier,
- f. dersom det er mulig, de planlagte tidsfristene for sletting av de forskjellige kategoriene av opplysninger,
- g. dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1.

## Kontroll på identiteter og tilganger

Det er viktig at kommunen har oversikt over hvilke brukergrupper, brukere og tilgangsbehov som finnes i en kommune. NSMs grunnprinsipper peker på at angripere ofte forsøker å få kontroll over brukerkontoer for å i neste omgang forsøke å øke tilgangen og rettighetsnivået til brukerkontoen. Dersom de lykkes med dette, kan angriperne ta seg lenger inn i systemet og få tilgang til flere ressurser. NSM viser videre til at mange virksomheter gir ansatte flere rettigheter enn de trenger, og at dette øker risiko for angrep. For å redusere risiko for angrep på kommunens IKT-systemer må kommunen derfor ha kontroll på brukernes kontoer og tilganger.

Tiltak for å sikre kontroll på identiteter og tilganger (prinsipp 2.6) er ifølge NSM å

- etablere retningslinjer for tilgangskontroll,
- etablere en formell prosess for administrasjon av kontoer, tilganger og rettigheter,
- benytte et sentralisert og automatiserbart verktøy for å styre kontoer, tilganger og rettigheter og å
- etablere multi-faktor autentisering.

### Sikkerhetsovervåkning

Et annet av NSMs prinsipper handler om å etablere sikkerhetsovervåkning (prinsipp 3.2.). Sikkerhetsovervåkning kan bidra til å oppdage sikkerhetshendelser tidlig, vurdere skadeomfang og hendelsens karakter og forstå hendelsesforløpet.

Videre anbefaler NSM at kommunen analyserer data fra sikkerhetsovervåkingen. Gjennom analyse av sikkerhetsrelevante data kan kommunen oppdage aktiviteter som påvirker informasjonssystemer, data og tjenester. NSM viser til at systematisert prosessering, gjennom sammenstilling og analyse av innhentet data vil bidra til å øke sannsynligheten for å avdekke hendelser.

### Inntrengingstester

NSMs grunnprinsipp 3.4 er å gjennomføre inntrengingstester for å oppdage og fjerne kjente sårbarheter og trusler. Det anbefales å gjennomføre inntrengingstester minst en gang i året. Kommunen bør ifølge grunnprinsippet jevnlig teste egen forsvarsevne for å verifisere etablerte sikkerhetstiltak, identifisere mangler og vurdere egen beredskap. Angripere utnytter ofte svakheter i virksomhetens rutiner.

### Databehandleravtaler

Personvernforordningen artikkel 28 stiller krav til kommunen knyttet til behandlinger av personopplysninger som skal gjøres av en databehandler på vegne av kommunen. Dersom en behandling av personopplysninger skal utføres på vegne av kommunen, skal kommunen bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen av personopplysningene oppfyller kravene i forordningen og vern av rettighetene til de som registreres.

Etter personvernforordningen artikkel 28 skal behandlinger utført av en databehandler være underlagt en avtale eller et annet rettslig dokument som er bindende for databehandleren med hensyn til den behandlingsansvarlige. Avtalen skal fastsette gjenstanden for og varigheten av behandlingen, behandlingens art og formål, typen personopplysninger og kategorier av registrerte, samt den behandlingsansvarliges rettigheter og plikter (artikkel 28 tredje punkt).

Datatilsynets veileder om virksomhetens plikter under personvernforordningen beskriver nærmere hva en databehandleravtale må inneholde i henhold til artikkel 28. Databehandleravtalen må inneholde:

- En beskrivelse av selve behandlingen av personopplysninger, herunder:
  - hva databehandleren faktisk skal gjøre
  - hva som er formålet med behandlingen
  - hvor lenge avtalen skal vare
  - hva slags personopplysninger som er registrert
  - hvilke kategorier av personer personopplysningene gjelder
- Pliktene og rettighetene til den behandlingsansvarlige, herunder å regulere følgende:
  - Den behandlingsansvarlige er ansvarlig for at personopplysninger blir behandlet i samsvar med personvernforordningen og personopplysningsloven (jf. artikkel 24).

- Den behandlingsansvarlige har både en rett og en forpliktelse til å bestemme hvilke formål, og hvilke hjelpemidler som kan brukes i behandlingen (jf. artikkel 4 nr. 7).
- Den behandlingsansvarlige skal gi databehandleren dokumenterte instruks for hvordan personopplysninger skal behandles (jf. artikkel 28 nr. 3 bokstav a). Instruksene skal være en del av avtalen eller lagt ved som et vedlegg til avtalen.
- Den behandlingsansvarliges rett til å si opp avtalen dersom databehandleren ikke lenger oppfyller lovens krav etter artikkel 28 nr. 1.
- Databehandlers forpliktelser, herunder:
  - bare behandle personopplysninger etter skriftlig instruks fra den behandlingsansvarlige
  - plikt til at autoriserte personer behandler personopplysningene fortrolig
  - plikt til å ha tilfredsstillende sikkerhetstiltak
  - bruk av annen databehandler (underleverandør)
  - bistand til å svare på anmodninger som gjelder de registrertes rettigheter
  - bistand til den behandlingsansvarlige
  - avslutning av avtalen
  - tilgjengeliggjøring av informasjon for den behandlingsansvarlige

### Opplæring i informasjonssikkerhet

NSMs veileder for «Grunnprinsipper for sikkerhetsstyring» (2020) viser til at ledelsen bør sikre tilstrekkelig risiko- og sikkerhetsforståelse i hele virksomheten. Dette gjøres gjennom opplæring av egne ansatte, samt å sørge for at leverandører, underleverandører og andre oppdragstakere har god risiko- og sikkerhetsforståelse. Ifølge NSM kan manglende opplæring bidra til sårbarheter, eksempelvis svak forståelse blant medarbeiderne om hvorfor sikkerhet er viktig for virksomheten, og manglende kunnskap om hvordan den enkelte kan bidra til god sikkerhet.. Dette er forhold som en trusselaktør kan utnytte til å påvirke virksomhetens verdier.

I KS sin veileder *Kommunedirektørens verktøykasse for informasjonssikkerhet* påpekes det at god informasjonssikkerhet til syvende og sist avhenger av ferdighetene og kunnskapen til menneskene i organisasjonen. Det er ifølge veilederen viktig at alle ansatte bidrar til at teknologi brukes riktig, prosesser følges, taushetsplikt ivaretas og at avvik knyttet til sikkerhet og personvern registreres og følges opp. I veilederen understrekes viktigheten med tilstrekkelig opplæring i alle ledd i kommunen. I veilederen anbefales kommunedirektøren å ha et opplæringsprogram hvor alle ansatte bevisstgjøres på hvordan kommunen skal ivareta god informasjonssikkert og godt personvern, og hva dette betyr for den enkelte. Kunnskap er ferskvare og opplæringen bør tilpasses den enkeltes stilling.

[Datatilsynet](#) skriver at målet med brukeropplæring er å sørge for at brukerne er oppmerksomme på trusler mot personvernet og informasjonssikkerheten generelt. Brukerne må være gitt muligheten til å etterleve dette i sitt daglige arbeid gjennom tilpasset opplæring ut fra behovet. Brukerne bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle risikoer.

Følgende revisjonskriterier legges til grunn for problemstilling 2:

| Problemstilling 2                                                                                                       | Krav og forventninger til kommunen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Har kommunen sørget for at personopplysninger som lagres i kommunens IT-systemer er sikret i tilstrekkelig grad?</p> | <p>Kommunen skal ha</p> <ul style="list-style-type: none"><li>→ internkontroll med personvern og informasjonssikkerhet, herunder<ul style="list-style-type: none"><li>○ styrende dokumenter for informasjonssikkerhet og personvern</li><li>○ tydelig rolle- og ansvarsfordeling knyttet til personvern</li><li>○ gjennomføre ledelsens gjennomgang</li></ul></li><li>→ protokoll over hvilke personopplysninger kommunen behandler (behandlingsprotokoll)</li><li>→ dokumenterte rutiner som bidrar til å sikre kontroll på identiteter og tilganger</li><li>→ etablert sikkerhetsovervåkning, og det bør gjennomføres analyser av data fra overvåkingen</li><li>→ gjennomført inntrengingstester jevnlig</li><li>→ rutiner og praksis som bidrar til å sørge for at kommunen har databehandleravtaler med eksterne leverandører som behandler personopplysninger</li><li>→ tiltak som sikrer at ansatte får opplæring i personvern</li></ul> |